**Open Source Solution Technology** 

# Active Directoryはもういらない!! Samba4最新情報



55 Terh

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

Copyright © 2009 Open Source Solution Technology

- 1 -



目次

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





- 3 -

## 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)

\$ 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
# 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

127.0.0.1localhost.localdomain localhost10.0.102.15samba4-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

Copyright © 2009 Open Source Solution Technology

/ -



# 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



# 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

# **Iusr/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

# **/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

	Ара	che Directory Studio	E	. 🗆 🗙
<u>File Edit Navigate LDAP Window Help</u>				
] 📬 🔒 🚔 ] 🖋 ] 🗇 🗘				
👫 LDAP Browser 🛛 🧟 🖉 🗖 🗖	📾 Entry Editor 😫	- 8	E Outline	
	DN: CN=Users,DC=samba4,DC=	=lan,DC=osstech,DC= ≅ ≅ 🗙 🔆 🗞 🖗 🗈 🖻 ‡ 🌣	⊂ CN=Users,DC=samba4,DC=lan,DC	C=osstec
	Attribute Description	Value	$\Rightarrow \equiv parentGUID (1)$	
▼ Z Root DSE (6)	objectClass	container (structural)	$\Rightarrow \equiv \text{objectClass}(2)$	
CN=Configuration,DC=samba4,DC=lan	objectClass	top (abstract)	$\Rightarrow \equiv \text{objectCategory}(1)$	
	cn	Users	$\triangleright \equiv cn(1)$	
CN=Builtin	instanceType	4	$ial \equiv nTSecurityDescriptor (1)$	
CN=Computers	nTSecurityDescriptor	00	$\triangleright \equiv \text{showInAdvancedViewOnly}(1)$	
B OU=Domain Controllers	objectCategory	CN=Container.CN=Schema.CN=Configuration.DC=sam	$\triangleright \equiv distinguishedName (1)$	
CN=ForeignSecurityPrincipals	description	Default container for upgraded user accounts	$\triangleright \equiv$ whenChanged (1)	
CN=Infrastructure	distinguishedName	CN=Users,DC=samba4,DC=lan,DC=osstech,DC=co,DC=ip	$\triangleright \equiv$ whenCreated (1)	
CN=LostAndFound	isCriticalSystemObject	TRUE	$\Rightarrow \equiv isCriticalSystemObject (1)$	
P @ CN=NTDS Quotas	name	Users	$\Rightarrow \equiv \text{description} (1)$	
CN=Program Data	objectGUID	Invalid Data	$\triangleright \equiv objectGUID (1)$	
CN=System	parentGUID	Invalid Data	$\triangleright \equiv uSNChanged$ (1)	
CN=Users (19)	replPropertyMetaData	Invalid Data	$\triangleright \equiv uSNCreated$ (1)	
CN=Administrator	showInAdvancedViewOnly	FALSE	$\triangleright \equiv systemFlags (1)$	
CN=Cert Publishers	systemFlags	-1946157056	InstanceType (1)	
CN=Certificate Service DCOM Ac	uSNChanged	3088	▷ ≡ name (1)	
CN=Cryptographic Operators	uSNCreated	3088		
CN=Domain Admina	whenChanged	2009/11/13 16:19:12 JST (20091113071912.0Z)		
CN-Domain Admins	whenCreated	2009/11/13 16:19:12 JST (20091113071912.0Z)		
CN-Domain Controllers				
CN=Domain Guests				
				>
🕼 Connections 🛛 🔐 Servers 🗖 🗖			C Progress 🙀 🏹	~
🕼 🔌 🗈 E	🗐 Modification Logs 🛛 🗐 Sea	irch Logs 🛛 💥 🛷 🗘 🕹 🖬 🌄 🗖 🗖	Open Connection (Finished at 16:39) Error while open S LOGON FAILURE	ж
🔓 Idap1		A		
🔩 samba4				
	<u>س</u> ر			
	98			



- 23 -

## 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

コンピューター名/ドメイン名の変更	
このコンピューターの名前とメンバーシップを変更できます。変更 ワークリソースへのアクセスに影響する場合があります。詳細情	Windows セキュリティ
コンピューター名(C): 🔓 yasumaWIN7	コンピューター名/ドメイン名の変更 ドメインに参加するためのアクセス許可のあるアカウントの名前とパス ワードを入力してください。
フル コンピューター名: yasumaWIN7SAMBA33 所属するグループ ③ ドメイン(D): samba4.lan.osstech.co.jp	Administrator       コンピューター名/ドメイン名の変更         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
○ 9-99)+-7(₩):	OK
ОК	*ンセル OK



## 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



- 24 -



- 25 -

# 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」

	とセキュリティ ▶ 管理ツール ▶	<b>-</b> 4 <sub>7</sub>	管理ツールの検索		Q
整理 ▼				= - 1	0
☆ お気に入り	名前	更新日時	種類	サイズ	-
📕 ダウンロード	🎴 リモート デスクトップ サービス	2009/11/06 18:10	ファイル フォル		
■ デスクトップ	■ Active Directory サイトとサービス	2009/11/06 18:10	ショートカット	2 KB	
◎ 最近表示した場所	■ Active Directory ドメインと信頼関係	2009/11/06 18:10	ショートカット	2 KB	
ACCESSION OF CHIMIN	🛜 Active Directory ユーザーとコンピュ	2009/11/06 18:10	ショートカット	2 KB	
	ੋ Active Directory 管理センター	2009/11/06 18:10	ショートカット	2 KB	=
	📝 ADSI エディター	2009/11/06 18:10	ショートカット	2 KB	
■ ドキュメント	キュリティ 、管理ツール 、       49       管理ツールの様         前       更新日時       種類         リモート デスクトップ サービス       2009/11/06 18:10       ファイル フォ         Active Directory サイトとサービス       2009/11/06 18:10       ショートカッ         Active Directory ドメインと信頼関係       2009/11/06 18:10       ショートカッ         Active Directory 管理センター       2009/11/06 18:10       ショートカッ         Active Directory 管理センター       2009/11/06 18:10       ショートカッ         Active Directory 管理センター       2009/11/06 18:10       ショートカッ         DFS の管理       2009/11/06 18:10       ショートカッ         DFS の管理       2009/11/06 18:10       ショートカッ         SCSI イニシエーター       2009/11/06 18:10       ショートカッ         SCSI イニシエーター       2009/11/06 18:10       ショートカッ         Windows PowerShell Modules       2009/07/14 13:52       ショートカッ         Windows メモリ診断       2009/07/14 13:41       ショートカッ         Windows メモリ診断       2009/07/14 13:41       ショートカッ         マンターネット インフォメーションサー       2009/07/14 13:41       ショートカッ         マンターネット インフォメーションサー       2009/07/14 13:41       ショートカッ         Windows メモリ診断       2009/07/14 13:41       ショートカッ         マンターネット インフォメーションサー       2009/07/14 13:41       ショートカッ         マンターネット インフォットションサー       2009	ショートカット	2 KB		
🔤 ピクチャ	🛃 DHCP	2009/11/06 18:10	ショートカット	2 KB	
🛃 ビデオ	🛃 DNS	2009/11/06 18:10	ショートカット	2 KB	
🎝 ミュージック	📷 Hyper-V マネージャー	2009/11/06 18:10	ショートカット	2 KB	
	🔝 iSCSI イニシエーター	2009/07/14 13:41	ショートカット	2 KB	
■ コンピューター	😹 SAN 用記憶域マネージャー	2009/11/06 18:10	ショートカット	2 KB	
	😹 Windows PowerShell Modules	2009/07/14 13:52	ショートカット	3 KB	
	溕 Windows PowerShell 用の Active Dir	2009/11/06 18:10	ショートカット	2 KB	
🖤 ネットワーク	ᡖ Windows システム リソース マネージ	2009/11/06 18:10	ショートカット	2 KB	
	📧 Windows メモリ診断	2009/07/14 13:41	ショートカット	2 KB	
	🛃 イベント ビューアー	2009/07/14 13:42	ショートカット	2 KB	
	🔊 インターネット インフォメーション サ	2009/11/06 18:10	ショートカット	2 KB	
	î オンライン レスポンダー管理	2009/11/06 18:10	ショートカット	2 KB	-
- 38 個の頂日	െലം എല്ലം കണ്ണ	0000 /44 /05 40 40	~	a. 178	Ţ
38 100 HE					



## Active Direcotry ユーザーとコンピューター

- ユーザー作成、グループ作成、OU作成など問題なし

● ユーザー管理

#### 新しいオブジェクト - ユーザー × 作成先: samba4.lan.osstech.co.jp/Users 姓(L): 竹内 名(F): 英雄 イニシャル(①): フル ネーム(A): 竹内 英雄 ユーザー ログオン名(U): takeuchil @samba4.lan.osstech.co.jp Ŧ ユーザー ログオン名 (Windows 2000 より前)(W): SAMBA4¥ takeuchi < 戻る(B) )次へ(N) > キャンセル



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 ポリシー管理エディター			- • •
ファイル(F) 操作(A) 表示(V) ヘルプ(H)			
🗢 🄿 🔁 📰 😖 🛛 🖬 🛛 🝸			
🧾 一般社員用 [samba4-cent5.samba4.lan.osstech. 🔺	設定	状態	כא⊏
▲ 👰 コンピューターの構成	[]] [パスワードの変更] を削除する	有効	ເກເກ
▷ 📫 ポリシー	🗈 コンピューターのロックを削除する	未構成	ເດເດງ
	一    目 タスク マネージャーを削除する	未構成	เกมร์
▲ 18 ユーザーの構成	    目 ログオフを削除する	未構成	003
▲ 二 ボリシー 目			
▲ ● ソフトウェアの設定			
■ ソフトフェア インストール A I <sup>CE</sup> Windows の設定			
▶ ■ ヤキュリティの設定			
▶			
 加 ポリシー ベースの QoS			
▷ 🍘 Internet Explorer のメンテナンス			
⊿ 📔 管理用テンプレート: ローカル コンピュ			
▷ 📋 Windows コンポーネント			
⊿ 📋 コントロール パネル			
□ プログラム			
□ プログラムの追加と削除	<		•
	\ 拡張 入標準 /		
4 個の設定			

Copyright © 2009 Open Source Solution Technology

- 28 -



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

🏓 🗣   🞽 🖬   🔍   🚺 🖬	VASI				
▲ A フォレスト: samba4.lan.osstech.co.in	TASC 推西				
	194.安				
▷ □ サイト		公開キーのポリシー/証明書!	ナービス クライアント - 自動	登録の設定	非表示
■ グループ ポリシーのモデル作成		ポリシー		係参な GPO	
▲ 🔂 グループ ポリシーの結果		証明書の自動管理	有効	[ 既定の設定]	
😭 YASUWIN7 上の takeuchi		オプション	設: 設:	定	
		新しい証明書を登録し、 を更新し、保留中の証明 効した証明書を削除す。	期限の切れた証明書 無: 明書要求を処理し、失 る	効	
		Active Directoryからの 使用する証明書を更新	)証明書テンプレートを 無: および管理する	劾	
		証明書の有効期限通知を	表示 無効	[既定の設定]	
		する			
	12	理用テンプレート			非表示
		ローカル コンピューターから	取得したポリシー定義(ADMX)	)ファイルです。	
		システム/Ctrl + Alt + Del ス	<b>ナブション</b>		非表示
		ポリシー	設定	優势な GPO	
		[パスワードの変更]を削除	する 有効	一般社員用	
		システムノリムーバブル記憶域	へのアクセス		<u>非表示</u>
		ポリシー	設定	優勢な GPO	
		リムーバブル ディスク:読み クセス権の拒否	取りア 有効	一般社員用	





### 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







- 31 -

## 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

ADSI エディター					23
☑ ADSI エディター	名前	クラス	識別名	操作	
▲ 圓 既定の名前付けコンテキスト [samba4-cer ▲ 🎦 DC=samba4,DC=lan,DC=osstech,DC ▲ 🚆 CN=Users	CN=竹内 英雄	user	CN=竹内 英雄,C	OU=osstech 他の操作	•
CN=Domain Users CN=Domain Guests CN=Domain Computers CN=Domain Controllers	CN=竹内 英雄 のプロ 属性エディター セキ: 属性(B):	パティ リティ			•
CN=Administrator CN=Guest CN=krbtgt CN=Enterprise Admins CN=Schema Admins CN=Cert Publishers CN=Cort Publishers CN=Group Policy Creator Own CN=RAS and IAS Servers CN=Read-Only Domain Contrc CN=Enterprise Read-Only Don CN=Cryptographic Operators CN=Event Log Readers	属性         department         departmentNumbidescription         desktopProfile         destinationIndication         displayName         displayName      <	値       マイス未設定>       マイス未設設定>       マイス未設設定>       マイス未設設定>       マイスま設定       マイスま設定       マイスまた       マイスまた	雄.OU=osstech,DC=s	amba4,DC=lan,DC=o	
ADSI エディター 更新 ショートカット さ	新日時: 2 ガイズ: 1.26 KB	OK ¥	やンセル 適用	3(A) (A)	78





- 33 -

## 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=openIdap --server-role='domain controller' --slapd-path=/opt/osstech/sbin/slapd



- 37 -

## 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