

# **samba4**

## **Latest updates**

Simo Sorce  
Samba Team

idra@samba.org  
<http://samba.org/~idra>

# Stato Attuale

- Servizi implementati:
  - ◆ Server SMB (SMB2)
  - ◆ Portmap (MS-RPC, IDL)
  - ◆ Server NBT
  - ◆ Server Wins (Server Wrepld)
  - ◆ Server Kerberos (integrazione di Heimdal)
  - ◆ Server LDAP (CLADP, LDB, AD)
  - ◆ Server Web (SWAT2)



# Condivisione file e stampanti

- Il core di samba rimane sempre la condivisione di file e stampanti, il server SMB è stato il primo ad essere riscritto ed è stato utilizzato come modello per la realizzazione di una serie di librerie di supporto estensivamente utilizzate nel resto della suite
- Gestione asincrona degli eventi
- Separazione dei vari layer e realizzazione di codice generico per la gestione dei vari layer
- Testsuites e librerie client



# libcli

- In samba4 è presente una libreria client che implementa tutti gli aspetti dei protocolli SMB e MS-RPC
- È stato uno dei tasselli principali e fondanti del processo
- Grazie ad essa è possibile scrivere suite di test veramente potenti (es: gentest)
- È una libreria completamente rientrante, ad eventi, e asincrona
- Tutti i dati riguardanti la connessione e i suoi stati sono conservati in apposite strutture ad albero e gerarchiche
- Le strutture non vengono più condensate e ridotte come in samba3 e non si rischia quindi di perdere informazioni



# RPC

- MS-RPC: Microsoft Remote Procedure Call
  - ◆ basato sullo standard DEC/RPC di OpenGroup
  - ◆ utilizzato su SMB e raw TCP come trasporti primari ma si vede anche su HTTP e altri protocolli
- Le RPC sono l'equivalente di chiamate a funzione che vengono però eseguite su un'altro server
- In Samba4 è stato completamente reimplementato il sottosistema RPC e si utilizzano finalmente file IDL per la definizione delle interfacce RPC e non solo
- Implementato anche il server portmap per RPC over TCP
  - ◆ Porta 135



# IDL

- IDL: Interface Definition Language
- È un linguaggio che serve a descrivere interfacce e viene utilizzato per prototipare velocemente funzioni RPC.
- Microsoft non ha mai rilasciato i file IDL che descrivono le proprie RPC
  - ◆ È necessario fare network analysis per ricavare le IDL dalla loro rappresentazione “on the wire”
- In samba4 abbiamo creato il compilatore ‘pidl’
  - ◆ È scritto in perl
  - ◆ Ha funzionalità più estese del compilatore MS equivalente (MIDL)
  - ◆ È utilizzato per generare IDL anche per altre funzioni (NBT, EJS)



# Talloc: memoria di ferro!

- Talloc è il sistema di allocazione e gestione della memoria
- Sviluppato in samba4 e già backportato in samba3
- Sistema di gestione di blocchi di memoria referenziati, strutturati in modo gerarchico e forniti di distruttore.
- Ogni puntatore è un “memory context” che può avere figli o essere figlio di un altro context.

Esempio di allocazione e liberazione di memoria in samba4:

```
struct foo *X = talloc(mem_ctx, struct foo);
X->name = talloc_strdup(X, "foo");

do_something(X);

talloc_free(X);      /* libera sia X che X->name in cascata */
```



# GenSec Library

- GenSec sta per Generic Security Library
- È una libreria che permette di utilizzare in modo trasparente metodi di sicurezza per la comunicazione, senza che l'applicazione che la utilizza (e i suoi programmatori) debbano sapere come funzionano questi meccanismi
- Implementa:
  - ◆ NTLMSSP
  - ◆ SASL
  - ◆ GSSAPI
  - ◆ SPNEGO
  - ◆ SIGN e SEAL
  - ◆ SCHANNEL
  - ◆ ...





# Nuovo Strato VFS

- Con Samba3 si è dimostrata la potenza del sistema VFS ma esso ha anche mostrato i limiti della struttura interna del software
  - ◆ Il sistema VFS è posizionato DOPO la traduzione da CIFS a POSIX
  - ◆ Alcune informazioni vengono perse e non possono essere comunicate direttamente al filesystem
- In samba4 il VFS è stato riposizionato a livello superiore
- Nasce quindi NTVFS
  - ◆ VFS con semantiche NT e non Posix
  - ◆ Ogni chiamata SMB è mappata nel VFS
  - ◆ La traduzione CIFS->Posix è demandata ad uno specifico modulo
  - ◆ Si possono usare File System più funzionali/flessibili di quelli Posix



# NBT, Wins e Wrepld

- Grazie a PIDL e ad una estensione ad hoc è stato possibile riscrivere molto velocemente sia il server NBT che il server Wins. Essi non riesiedono più nel demone nmbd ma sono integrati in smbd
- È in fase avanzata di sviluppo anche wrepld il sistema di replicazione dei server WINS compatibile con i server WINS di Microsoft
  - ◆ Porta tcp 42



# LDAP Client e Server

- Per funzionare come DC Active Directory un protocollo fondamentale da supportare è LDAP sia client che server
- In Samba3 e 4 si è deciso di riscrivere le librerie LDAP (ildap) per problemi legati alle librerie di openLdap
- È necessario integrarsi con un server Ldap
  - ◆ il codice di openLdap è difficilmente integrabile con samba4
  - ◆ scrivere moduli è difficile per la scarsissima documentazione
- In Samba4 è stato scritto un server LDAP basato su LDB
  - ◆ ancora incompleto ma funzionante
- È implementato anche un server CLDAP
  - ◆ Porta 389 UDP

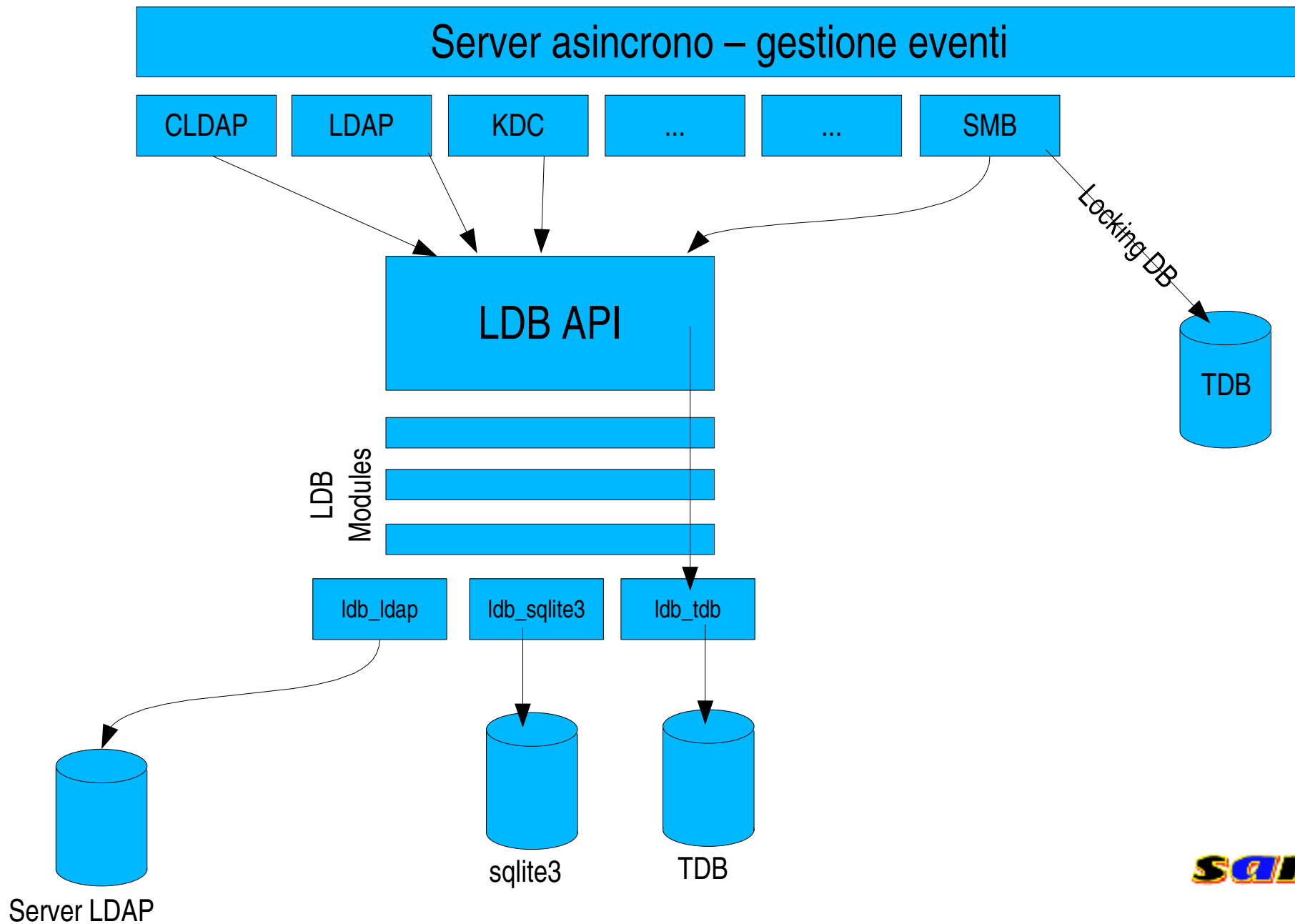


# LDB: LDAP like DB

- LDB è il successore di TDB
- LDB è un database gerarchico con una sintassi molto simile a LDAP
  - ◆ Sintassi basata su attributi, valori e DN
  - ◆ Assenza di schema
- LDB usa TDB o LDAP (o SQLITE3) come storage
  - ◆ L'uso di TDB lo rende estremamente performante
  - ◆ Quando si usa LDAP è necessario fornire uno schema
- È il sistema di salvataggio dati di riferimento per Samba4



# Samba e LDB



# TDB e transazioni

- Recentemente è stato aggiunto il supporto per le transazioni
- Binary compatible con il formato precedente
- Sempre Multiple-reader e Multiple-writer
  - ◆ Durante una transazione si può continuare a leggere il database ma non aggiornarlo
  - ◆ I dati che gli altri processi vedono durante una transazione sono consistenti, le nuove operazioni risultano visibili solo a conclusione della transazione



# Server Web

- Samba4 include swat2, un server web per la configurazione completa del sistema
- L'intenzione è quella di renderlo il sistema di default utilizzato per la configurazione fin dal momento zero dell'installazione
- Come progetto secondario scaturito dal server web è stato integrato EJS, un interprete che utilizza un linguaggio derivato da javascript
- EJS è la base di un sistema di scripting interno utilizzato sia nel server web che come tool per la creazione di suite di test



# Obiettivi

- Obiettivi Iniziali<sup>1</sup>:
  - ◆ Implementazione completa dei protocolli
  - ◆ Testabilità totale
  - ◆ non-POSIX backends
  - ◆ codice completamente asincrono
  - ◆ modello di processo flessibile
- Obiettivi attuali:
  - ◆ Completa compatibilità con Active Directory e Windows 2003 Server

1: [http://us2.samba.org/samba/ftp/slides/samba4\\_aaug.pdf](http://us2.samba.org/samba/ftp/slides/samba4_aaug.pdf)





# Active Directory ? Si, grazie

- Supporto completo ad Active Directory
- Comporta l'integrazione con:
  - ◆ Kerberos e DNS
  - ◆ LDAP e CLDAP
- È necessario:
  - ◆ Completo supporto a MS-RPC
  - ◆ Supporto di MS-RPC e SMB su più trasporti
  - ◆ Implementazione di altri protocolli e/o integrazione con altri progetti che già li implementano
  - ◆ Un server Kerberos
  - ◆ Un server LDAP
  - ◆ Un server DNS



# Posix o non-Posix

- Samba è nato per i sistemi tipo Unix e quindi Posix
- Problema:
  - ◆ Le semantiche di Windows sono più ricche
  - ◆ Molte applicazioni cominciano a dipendervi
  - ◆ Esempio più evidente sono le ACL
- Soluzione:
  - ◆ Supportare anche FileSystem non-Posix
  - ◆ Supportare tutte le semantiche Windows
  - ◆ Permettere a terze parti di sfruttare File System più flessibili per essere più compatibili con semantiche non-Posix



# Process model

- Multi Tasking o Multi Threading ?
  - ◆ In samba3 più richieste su una singola connessione non possono essere evase contemporaneamente, il codice è bloccante e non funziona in modalità multithread
- Samba4 è pensato per poter funzionare con diversi modelli di processo
  - ◆ single (un solo processo per tutte le richieste)
  - ◆ standard (un task per client come Samba3)
  - ◆ thread (un pthread per client)
- Samba4 è inoltre completamente **asincrono** e utilizza una coda ad eventi per qualsiasi comunicazione



# Navigazione a ... Vista

- Dal rilascio di pochi giorni fa dell'ultima beta di Microsoft Vista è arrivata una novità: SMB2
- SMB2 è una nuova variante di SMB in cui è stata profondamente cambiata la struttura dei pacchetti
- Abbiamo già cominciato ad analizzare il protocollo e abbiamo già iniziato ad estendere la nostra libreria client in modo da supportarlo.
- Quando la libreria client sarà terminata lo adotteremo anche nel codice del server



# Conclusioni

Samba4 è ancora immaturo e può essere usato solo a scopo di test, ma lo sviluppo procede molto bene e abbastanza speditamente.

In tempi molto brevi saremo in grado di rilasciare la prima Technology Preview Release.

Se volete seguire e/o partecipare allo sviluppo collegatevi a <http://devel.samba.org> e seguite le istruzioni per scaricare l'albero SVN marcato con il tag *samba4* e iscrivervi alla mailing list [samba-technical@samba.org](mailto:samba-technical@samba.org) e/o collegarvi al canale IRC #samba-technical sui server FreeNode

Siti principali:

<http://www.samba.org>

<http://news.samba.org>

Mailing list di supporto utenti:

[samba@samba.org](mailto:samba@samba.org) (in inglese)

[samba-it@xsec.it](mailto:samba-it@xsec.it) (in italiano)

