uno sguardo al futuro

Simo Sorce
Samba Team

idra@samba.org

Obiettivi

- Obiettivi Iniziali[1]:
  - 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_auug.pdf

Supportare tutti i protocolli

- La suite di protocolli SMB/CIFS è molto vasta
- Protocolli principali
  - NetBIOS
  - SMB
  - MS-RPC
  - LDAP
  - Kerberos/DNS
- Fino a Samba3 la filosofia era quella di implementare lo stretto indispensabile
- In Samba4 l'obiettivo è quello di implementare tutto in modo completo

Testare, testare, testare, testare ...

- In Samba 3 erano disponibili una serie di tool di test ma con varie limitazioni:
  - incompleti o parziali
  - completi ma dedicati a poche, piccole porzioni dei vari protocolli
- Per raggiungere gli obiettivi di Samba4 è necessario:
  - testare tutti i protocolli
  - testare ogni aspetto dei singoli protocolli
  - impedire regressioni nel codice
  - verificare che l'implementazione di samba sia pienamente compatibile con client e server Windows

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 Sytem più flessibili per essere più compatibili con semantiche non-Posix

Process model

- Multi Tasking o Multi Threading ?
  - il vecchio codice è portabile ma non rientrante
  - non è possibile utilizzarlo in ambienti multithread
  - più richieste su una sinola connessione non possono essere evase contemporaneamente
- 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)

Parola d'ordine: asincrono

- La maggior parte del codice di Samba3 verrà riscritto
- Uno dei motivi fondamentali è che il codice è spesso bloccante
- Se samba sta elaborando una richiesta non può rispondere ad altre richieste
- Samba4 è già architettato in modo che tutte le richieste possano essere schedulate e messe in una coda ad eventi

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
  - Heimdal e MIT per Kerberos
  - openLdap* per LDAP
  - BIND come DNS Server

Stato Attuale

- Architettura
- Funzionalità:
  - Talloc
  - LDB
  - (MS)RPC
  - IDL
  - Raw Client Library
  - NTVFS
  - cifs vfs, tank vfs e posix vfs
  - gensec
  - LDAP
  - ACL e linux security module

Architettura

- Samba4 è una completa riscrittura “from scratch” del codice.
- Con Samba4 si ha una chiara separazione dei layer (netbios,smb,rpc) eliminando la commistione di protocolli presente nelle precedenti versioni.
- Il flusso di dati è gestito da una coda di richieste e risposte in entrata e uscita con la possibilità di essere eseguito in modo asincrono
- Inoltre è possibile utilizzare diversi modelli di processo utilizzando il più adatto al compito da svolgere. Esempio:
  - single per embedded
  - thread per file server utilizzati con Terminal Server
  - standard per il normale utilizzo

Talloc: memoria di ferro!

- Talloc è il sistema di allocazione e gestione della memoria
- In samba4 è stato completamente rivisto ed è molto cambiato da quando voleva dire: “trivial alloc”
- Ora è un sistema di gestione di blocchi di memoria referenziati, strutturati in modo gerarico e forniti di distruttore.
- Praticamente ogni puntatore è un “memory context” che può avere figli o essere figlio di un altro context.

Esempio di allocazione di memoria in samba4:

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

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 come storage
  - L'uso di TDB lo rende estremamente performante
  - Quando si usa LDAP è necessario fornire uno schema
- Sta diventando il sistema di salvataggio dati di riferimento per Samba4

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 du HTTP e altri protocolli
- Le RPC sono l'equivalente di chiamate a funzione che vengono però eseguite remotamente (almeno concettualmente) su un'altro server
- Microsoft continua ad estendere la suite di protocolli CIFS aggiungendo nuove RPC ad ogni rilascio di un Sistema Operativo o di un Service Pack
- In Samba4 è stato completamente reimplementato il sottosistema RPC e si utilizzano finalmente file IDL per la definizione delle interfaccie RPC

IDL

- IDL: Interface Definition Language
- È un linguaggio che serve a descrivere interfacce e viene utilizzato per prototipare velocemente l'aspetto delle RPC senza preoccuparsi di come questo viene codificato in rete
- Microsoft non ha mai rilasciato i file IDL che descrivono le proprie RPC
  - È necessario fare network analisys per ricavare le IDL dalla loro rappresentazione sul cavo
- In samba4 è stato costruito un compilatore di IDL che si chiama pidl
  - È scritto in perl
  - Ha funzionalità più estese del compilatore MS equivalente (MIDL)
  - Può essere riutilizzato in altri progetti

Nuova libreria client

- In samba4 è già presente una libreria client che implementa tutti gli aspetti del protocollo smb e rpc
- È stato uno dei tasseli 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 engono più condensate e ridotte come in samba3 e non si rischia quindi di perdere informazioni

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 communicate 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
  - Non vi è perdita di informazioni
  - Si possono usare File System più funzionali/flesibili di quelli Posix

Moduli VFS

- Sono già disponibili diveris moduli VFS
- CIFS VFS
  - È un modulo “pass-through”
  - Permette di testare il codice interno di samba4 utilizzando un terzo server come “file system cifs”
- TANK VFS
  - È un modulo specializzato che utilizza direttamente lo storage Tank di IBM che ha più funzionalità dei Posix
- Posix VFS e unixuid
  - La compatibilità Posix non è più il paradigma di samba, ma è una delle sue componenti, questo rimarrà comunque la coppia di moduli più utilizzata in assoluto

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

LDAP Client e Server

- Per funzionare come DC Active Directory un protocollo fondamentale da supportare è LDAP sia client che server
- Samba3 utilizza le librerie openLdap per la connesione a server Ldap
  - openLdap server come storage per passdb
  - Active Directory quando è membro di un dominio AD
- In Samba3 e 4 si è deciso di riscrivere le librerie per problemi legati alle librerie di openLdap
- È necessario integrarsi con un server Ldap
  - al momento si utilizza openLdap per i test
  - il codice di openLdap è inutilmente troppo complesso
  - scrivere moduli è difficile per la scarsissima documentazione
- In Samba4 si sta scrivendo un server Ldap basato su LDB

ACL e LSM

- Uno dei problemi più sentiti è la scarsa compatibilità delle ACL Posix con quelle Windows
- Ciò rende la conversione tra le due semantiche insoddisfacente e complessa
- Samba però non si può occupare di autorizzare gli accessi
  - è compito del kernel
  - farlo in userspace è impossibile senza “races”
- Probabile soluzione: Linux Security Modules
  - Ogni chiamata a kernel che coinvolge le ACL viene intercettata
  - Vengono mantenute due sia le ACL Posix che Windows sul file attraverso Extended Attributes
  - Samba potrà accedere direttamente alle ACL Windows
  - LSM si occuperà di mantenere sincronizzati i due set di ACL facendo le opportune conversioni in modo race-free

Conclusioni

Samba4 è ancora immaturo e può essere usato solo a scopo di test, ma lo sviluppo procede molto bene e abbastanza speditamente.
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 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 (in inglese)
samba-it@xsec.it (in italiano)