

# Samba: presente e futuro

Simo Sorce  
Samba Team

[idra@samba.org](mailto:idra@samba.org)



# Presente: Samba3

- La versione corrente di samba è la 3.0.9 (è prevista un serie 3.2.x)
- Funzionalità:
  - File server
  - Print server
  - Wins server
  - Domain Controller NT4 compatibile
  - Domain Server
  - Domain Workstation (winbind)
- Lacune
  - Mancano tutti i protocolli di sincronizzazione “nativi”
  - Non è possibile avere DC misti MS+Samba
  - Non è possibile avere wins secondari



# Samba3 come File server

- Samba3 è un'ottimo file server
- Out of the Box ha dimostrato di essere più performante di windows 2003 sullo stesso hw
- Funzionalità
  - ◆ Tutte le normali operazioni sui file
  - ◆ Il layer VFS permette di estendere le funzionalità del fs
  - ◆ Unix Extensions
- Lacune
  - ◆ ACL mapping non perfetto
  - ◆ Manca il supporto per gli stream



# Samba3 come Domain Controller

- Supporta tutte le RPC necessarie ai client di un dominio, dalla 3.0.9 vi sono report che anche i server exchange (5.5 finora) funzionano correttamente in un dominio samba
- Non supporta la replicazione del SAM con DC Microsoft
- Si possono utilizzare più DC samba, ldap è il backend preferito in queste situazioni per le sue funzionalità di replicazione
- Sono supportati i gruppi (anche nested) e tutte le funzionalità di controllo account e password



# Migrazione a Samba

- Samba offre tool dedicati per migrare un intero server NT.
- Con il comando vampire del tool “net” è possibile replicare completamente il SAM di un server NT
- Con i comandi net rpc share e net rpc printer è possibile migrare stampanti e directory su un nuovo server
- In poche ore è quindi possibile sostituire un file/print/dc server NT con uno samba senza riconfigurare i client.



# Domain clients via samba

- Anche le macchine unix possono diventare client di dominio
- Tramite il demone winbind e i sistemi nsswith e pam è possibile ottenere le liste di utenti e gruppi e delegare la'utenticazione al dominio
- Tramite Cifsvfs (kernel 2.6) o smbfs (quasi obsoleto) è possibile utilizzare dischi remoti su server Windows o samba
- Se il controller è Active Directory è possibile usare kerberos per il Single Sign On



# Futuro: Samba4

**samba4**



# 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)





# Compatibilità completa

- La suite di protocolli SMB/CIFS è molto vasta
- Fino a Samba3 la filosofia era quella di implementare lo stretto indispensabile
- In Samba4 l'obiettivo è quello di implementare tutto in modo completo
- Anche a livello di file system si è deciso di elevare l'astrazione dal modello posix in modo da poter utilizzare filesystem custom che possano offrire tutta la semantica di CIFS/NTFS



# 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 singola 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)



# Active Directory ? Si, grazie

- Supporto completo ad Active Directory
- Comporta l'integrazione con:
  - ◆ Kerberos, DNS, LDAP, CLDAP, ecc..
- È necessario:
  - ◆ Completo emulazione di tutte le RPC IN PROGRESS
  - ◆ Supporto di MS-RPC e SMB su più trasporti OK
  - ◆ Implementazione di altri protocolli e/o integrazione con altri progetti che già li implementano ATTIVO
    - Heimdal e MIT per Kerberos
    - openLdap\* per LDAP
    - BIND come DNS Server

\*openldap potrebbe venire sostituito da un server ldap interno a samba4



# Stato Attuale

- Architettura
- Funzionalità:
  - ◆ Foundation Libraries
    - Talloc
    - LDB
    - IDL Compiler
  - ◆ Subsystems
    - (MS)RPC
    - 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



# 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
  - ◆ 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



# 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 connessione 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](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)



# Contatti

Offro supporto professionale tramite Xsec srl, società che ho fondato insieme ad altri soci a Milano.



**via Garofalo 39, Milano**  
**Tel. 0229534143****Sito.**  
<http://www.xsec.it/>  
**Mail. info@xsec.it**

Xsec partecipa attivamente al Consorzio CIRS che permette di ottenere supporto alla migrazione su gran parte del territorio nazionale



**via Gaeta 16, 00185 Roma**  
**Tel. 064404656**  
**Sito. [www.consorziocirs.it](http://www.consorziocirs.it)**  
**Mail. info@consorziocirs.it**

