Samba, opening windows to a wider world

Simo Sorce -- idra@samba.org
Samba Team -- http://www.samba.org

Cosa e‘ Samba?

- Samba e‘ l’implementazione di un Server SMB
  - SMB (o CIFS) e‘ il protocollo di condivisione delle risorse usato dai client Microsoft
- Iniziato nel 1991 da Andrew Tridgell
- Samba e‘ Software Libero distribuito con licenza GPL
- Supporta molte piattaforme
  - Linux, Solaris, HP-UX, AIX, True64, *BSD, e altre ancora

Dove trovo Samba?

- all’indirizzo http://www.samba.org si trova una lista di mirrors da cui scaricare l’ultima versione.
- Scegliete il mirror a voi piu‘ vicino.
- Sono disponibili anche pacchetti binari per alcune distribuzioni linux.

Dove trovo documentazione e aiuto?

- Documentazione
  - http://www.samba.org/samba/docs/index.html
  - Samba-HOWTO-Collection.pdf
  - sottodirectory /docs nell’archivio col codice sorgente

- Aiuto
  - samba@samba.org (mailing list)
  - http://www.samba.org/samba/support/index.html (lista di aziende che offrono supporto commerciale)

Chi sviluppa Samba?

Il Team Samba e‘ un gruppo di circa 20 persone (6-8 attive) sparse per tutto il mondo che contribuiscono allo sviluppo di Samba.

Lo sviluppo viene coordinato tramite la mailing list samba-technical@samba.org aperta a chiunque.

Se desiderate contribuire al progetto, il primo passo e‘ l’iscrizione a questa lista. (http://lists.samba.org)

Qui potete trovare la lista aggiornata dei membri attuali: http://www.samba.org/samba/team.html

Cosa e’ Samba? Il protocollo SMB/CIFS

- Il protocollo NetBIOS
  - Da dove viene?
  - NetBIOS su TCP/IP
  - Samba e NetBIOS
- Il protocollo SMB/CIFS
  - Server Message Block/Common Internet File System
  - "windows on the wire"
  - Protoccolo di condivsione delle risorse
  - Scherzosamente:
    - Common Insecurities Fail Scrutiny

NetBIOS, da dove viene?

- Discende dal Manuale dell'IBM
  - Network Technical Reference Manual Sept. 1984
- NetBIOS su TCP/IP (NBT)
  - RFC 1001/1002
- Fornisce 3 servizi
  - Name service (udp/137)
  - Message service (udp/138)
  - Session service (tcp/139)
- NetBIOS non fornisce condivisione delle risorse

NetBIOS, a cosa serve?

- Il Name Service e’ analogo al DNS
  - Nome di 15 caratteri piu’ 1 che identifica il tipo di risorsa
  - Il nome viene richiesto dai client
  - Chi ha un nome deve "difenderlo"
  - Non e’ molto sicuro...
- Il Message Service
  - Servizio di Messaging (es. winpopup)
- Il Session Service
  - Necessita il nome NetBIOS del chiamante e del chiamato per stabilire una connessione statefull
  - E’ il trasporto per CIFS(SMB)

NetBIOS: note

- I client Windows incapsulano NetBIOS su piu‘ protocolli (IPX/SPX, TCP/IP, NetBEUI)
  - Samba utilizza solo NetBIOS su TCP/IP
  - E’ altamente sconsigliato utilizzare NetBIOS su piu‘ protocolli contemporaneamente.
- Windows 2000 permette di utilizzare CIFS direttamente sulla porta tcp/445
  - NetBIOS-less CIFS
  - Samba supporta questa modalita’ solo nel branch di sviluppo

CIFS (Common Internet File system)

- Permette la condivisione di files...
  - permessi sulle share
  - permessi sui file
  - locking dei file
- ...e stamapanti
  - Se l'OS ci puo' stampare allora posso farlo anch'io
  - sistemi di stampa supportati:
    - BSD(default), AIX, LPRNG, HP-UX, PLP, QNX, SOFTQ, SYSV, CUPS

Novita‘ nella serie 2.2.x

- Supporto per le RPC di stampa di Windows NT 4.0
  - Point & Print per Windows 9x/NT/2000
  - ACL sulle code di stampa
- Supporto per la manipolazione delle ACL sul sistema server tramite la shell grafica di Windows (WinNT Explorer)
  - necessita un file system che supporti le ACL
    - --with-acl-support
  - ACL sulle share
- Semantica interna del locking riscritta
- Supporto ufficiale come controller di domini
  - Supporta Win NT 4 e 2000 come membri di dominio
  - Fornisce le liste di utenti ai client Win 9x
  - Non supporta ancora la funzionalita‘ BDC

Novita‘ nella serie 2.2.x (continua)

- Winbind (dalla versione 2.2.2)
- Supporto per funzionare come MS-DFS server
  - --with-msdfs
- Nuovo VFS layer
  - --with-vfs
- Molti database interni ora in formato TDB
  - piu‘ veloce
  - piu‘ efficiente
- Supporto PAM migliorato
  - --with-pam

Point & Print

- Samba 2.2 da‘ la possibilita‘ di fornire automaticamente i driver delle stampanti ai client Windows on-demand
- I driver delle stampanti devono essere prima "installati" e assegnati alle stampanti sul server Samba
  - Windows NT 4.0 Add Printer Wizard (APW)
  - Imprints toolset
    - http://imprints.sourceforge.net
- La versione 2.2.0 di Samba ha un bug che obbliga ad avere il driver installato prima di usare APW sui client NT, dalla 2.2.1 si puo‘ utilizzare APW da client 9x/NT/2000 per installare un driver per la stampante sul server Samba.

Access Control Lists

- Samba 2.2 introduce la possibilta‘ di manipolare le Access Lists del filesystem attraverso la Windows NT Explorer security tab.
  - Ogni sistema ha una propria implementazione delle ACL
  - Richiede che venga scritto un supporto specifico per ogni implementazione
    - Attualmente disponibile per: Linux ext2(3)+bestbits patch, Linux+XFS, Solaris, IRIX, AIX, Tru64, Unixware ...
- Viene fatto un mapping tra ACL di NT e POSIX ACL
  - campi semantici differenti (ALLOW, DENY)
  - permessi mappati (R,W,X e O)
- le ACL sulle share sono salvate in un TDB
  - non e‘ necessario --with-acl-support

Locking

- exclusive locks
  - solo l’applicazione che ha il lock puo’ leggere/scrivere
- batch oplocks
  - il client SMB mantiene il lock anche dopo che l’applicazione l’ha rilasciato, in caso che ne abbia di nuovo bisogno
- level 2 oplocks
  - permette al client di passare (downgrade) da lock esclusivo a lock a sola lettura

Locking: opzioni di controllo in smb.conf

- kernel oplocks (boolean, global)
  - supportato da IRIX (6.5.2f) e Linux (2.4).
- locking (boolean)
  - controlla se il server esegua richieste di lock su un blocco di byte; se disabilitato tutte le richieste sembreranno andare a buon fine.
- oplocks (boolean)
  - disabilitarlo puo' ridurre le prestazioni fino al 30%.
- level2 oplocks (boolean)
  - da utilizzare quando non si deve scrivere sui file.
- strict locking (boolean)
  - controlla il lock prima di ogni singola lettura/scrittura

Domini Windows NT 4.0

- Samba e‘ in grado di partecipare come membro di dominio di un vero dominio Windows NT 4.0
- Essere membro di un dominio e‘ meglio che utilizzare la modalita‘ di sicurezza "server" (opzione: security = server)
  - Usa meno risorse sul DC
  - Puo‘ utilizzare le Domain Trust Relationships
- E‘ sempre necessario che ad ogni utente NT sia associato un utente del sistema
  - winbindd
  - pam_winbind.so
  - nss_winbind.so

Domini Windows NT 4.0 (continua)

- Supporto ufficiale come Domain Controller nella versione 2.2
  - Liste utenti per Windows 9x
  - completo supporto client Windows NT 4.0 SP3+
  - supporto client Windows 2000 in modalita‘ legacy
- Le System Policy funzionano allo stesso modo che nei domini Windows NT 4.0
  - eccezion fatta per i gruppi, il cui supporto verra‘ probabilmente aggiunto in una delle prossime release della serie 2.2
- Non supporta le Trust Relationship con altri domini
- Non supporta ancora il protocollo di replicazione con altri DC Windows NT 4.0
  - non puo‘ essere o avere BDC (*)

MS-DFS

- MS Distributed File System
  - redirige le richieste di un client verso una share su altri server.
  - la comunicazione passa sempre attraverso il server samba.
  - supporta nativamente:
    - Windows 98/ME
    - Windows NT 4.0
    - Windows 2000
- host msdfs (boolean, global)
  - attiva/disattiva supporto ms-dfs
  - (e' comunque necessario compilare con --with-msdfs)
- msdfs root (boolean, share)
  - indica che la share puo' contenere redirezioni

ln -s msdfs:server\\share[,server\\share] dirname

es: cdrom -> msdfs:winserver\cdrom

Internals...

- VFS - Virtual File System Layer
  - Dalla versione 2.2 tutte le operazioni sul filesystem sono state raccolte nel VFS ed e' stata creata una API per permettere l'uso di moduli aggiuntivi (es: auditing)
- TDB - Tiny Data Base
  - Per ottimizzare alcune operazioni abbiamo introdotto l'uso di un database molto semplice, ma veloce; utilizziamo tdb sia per dati temporanei (es: lock db) che per dati permanenti (es: driver stampanti).
- PAM - Pluggable Authentication Module Support
  - E' supportato l'uso di PAM per armonizzare la gestione degli account (policy enforcement) ed e' anche possibile utilizzarle per l'autenticazione quando si usano password in chiaro.

passdb - storage informazioni utenti

- Lo storage delle informazioni degli utenti e’ stato astratto in un interfaccia modulare (a breve caricabile dinamicamente)
- Sono stati implementati i seguenti moduli per il salvataggio delle informazioni relative agli utenti (username, password, home directory, logon script ...
  - pdb_smbpasswd (classico file di testo)
  - pdb_tdb (basato su tdb)
  - pdb_ldap (basato su OpenLdap)
  - pdb_nisplus (tabelle nis+)
- Scrivere un nuovo modulo per il salvataggio delle informazioni non e’ difficile, ci sono progetti per la realizzazione di un modulo che salvi su database SQL.

Samba 3.0

- Unicode
  - Gradualmente si sta convertendo tutto il codice ad utilizzare solo caretteri unicode a 16bit.
- Replicazione PDC/BDC
  - E’ previsto il supporto PDC/BDC con replicazione nativa per domini NT
- Active Directory / Kerberos
  - Gia’ ora il branch HEAD di sviluppo (samba 3.0alpha*) supporta AD e Kerberos, al momento samba e’ in grado di essere server membro di realm kerberos(AD), e i client possono autenticarsi con kerberos. In futuro: trust rel. e samba come KDC.

Risorse

- Roadmap & Release Plans
  - http://www.samba.org/samba/development.html
- TODO list e progetti aperti
  - http://www.samba.org/samba/TODO.html
- Risorse per gli sviluppatori
  - http://www.samba.org/samba/devel-links.html
- Sito Principale
  - http://www.samba.org/
- Mailing Lists
  - http://lists.samba.org/