Breve guida utente AFS

AFS (Andrew File System) e' un file system distribuito con un name space comune.
Basato su un modello architetturale client/server, consente ad uno o piu' client di accedere ai file resi disponibili da uno o piu' file-server.

Come il file system Unix, AFS utilizza per i file una struttura gerarchica ad albero. Per convenzione la root directory del file system e' identificata da `/afs`, mentre le subdirectory della root definiscono le celle del file system AFS. Una cella e' un dominio amministrativo nello spazio AFS, al quale afferiscono l'insieme di client e server.
Un meccanismo di caching, attivo su ogni client, consente una maggiore velocita' nell'accesso ai file, preoccupandosi di mantenere su un disco locale una copia dei file in uso su quel determinato host.

Lo spazio disco sui file server AFS e' organizzato in volumi: contenitori di file e directory resi disponibili all'utente come una sottodirectory dell'albero AFS. Ogni volume ha definita una *quota*, assegnata dall'amministratore locale, che definisce la quantita' massima di dati che un volume puo' contenere.
L'home directory di ogni utente nella cella *infn.it* risiede su un differente volume.

Dal punto di vista dell'utente la natura distribuita del file system, dei volumi e del sistema di caching, e' assolutamente trasparente, non essendo visibili i riferimenti ai server e quindi alla locazione fisica dei file. A partire dalla root directory `/afs`, l'utente vedra' la stessa struttura di directory su tutti gli AFS client.

Security in AFS

Tra i diversi metodi insiti nella tecnologia AFS per il controllo dell'accesso allo spazio disco distribuito, quelli di maggior interesse per l'utente finale sono l'Autenticazione e le ACL.

Autenticazione

Per accedere allo spazio AFS ogni utente deve essere autenticato, questo e' normalmente effettuato al login time, fornendo una password associata alla propria username: in questo modo l'utente ottiene un *token*, che verra' automaticamente distrutto al logout.
Il *token* ha definito per default un lifetime di 24 ore, trascorse le quali l'utente non sara' piu' in grado di accedere ai relativi files in AFS. Il comando `klog` permette all'utente di ottenere un nuovo *token* senza dover aprire una nuova sessione di lavoro.

ACL

Ogni directory in AFS ha definite delle ACL (Access Control List). Le ACL non possono essere definite per singoli files, e' opportuno quindi organizzare il proprio spazio disco tenendo presente che files presenti in una stessa directory avranno definite uguali protezioni.

Le ACL possono essere applicate ad utenti o a gruppi, garantendo o negando ogni combinazione di diritti di accesso alle directory e quindi ai file in esse contenuti.
Una *user entry* si applica solo al corrispondente utente, una *group entry* si applica a tutti i membri di quel dato gruppo. Un gruppo puo' consistere di un insieme di utenti, macchine e network, queste ultime due individuate attraverso il loro indirizzo IP.
Se un utente e' membro di un gruppo o e' collegato su una macchina membro di un gruppo, l'utente acquisisce i diritti assegnati a quel gruppo .

Esistono dei gruppi predefiniti, tra i piu' importanti nella cella *infn.it* troviamo:

system:anyuser	→	chiunque collegato su un client afs nel mondo
system:authuser	→	tutti gli utenti autenticati nella cella *infn.it*
infn:nodes	→	elenco degli host e/o network INFN

E' possibile per l'utente definire fino a 20 nuovi gruppi, a cui assegnare diritti in una determinata directory. Il nome di un gruppo sara' nella forma *owner:group* (es: *pippo:amici*).
Ogni utente puo' definire proprie ACL per lo spazio disco che amministra, ricordando che, a differenza del file system Unix, in AFS tutti i file in una directory sono soggetti alle stesse restrizioni. Inoltre, sebbene le classiche protezioni Unix siano visibili, in un file system AFS queste sono trattate diversamente: hanno effetto solo i bit relativi all'owner del file.

Home directory Backup

Per tutti i volumi della cella AFS *infn.it* gestiti dai server *afsitfs1* e *afsitfs2* e' previsto un backup incrementale giornaliero su base mensile.
E' inoltre disponibile in linea un volume di backup delle home directory degli utenti della cella *infn.it*, aggiornato alla sera precedente. Questi volumi sono accessibili a tutti gli utenti come `/afs/infn.it/backup/user/[a-z]/$USER` .
E' tuttavia possibile montare il proprio volume di backup, anche in una qualsiasi altra directory in cui si abbiano i privilegi di Administer, Insert e Delete, con il seguente comando:

```
fs mkmount -dir <directory> -vol <volume name>
```

eg: `fs mkmount -dir tempbck -vol user.$USER.backup`
(l'utente `$USER` monta il proprio volume di backup, nella directory `tempbck`)

Dopo aver recuperato dal volume di backup i file di proprio interesse, si puo' rimuovere il mount-point:

```
fs rmmount -dir <directory>
```

eg: `fs rmmount -dir tempbck`
(l'utente `$USER` smonta il proprio volume di backup, dalla directory `tempbck`).

Principali comandi AFS

Comandi base:

`kpasswd`	equivalente del comando Unix `passwd`, consente di cambiare la propria password AFS;

`tokens`	permette controllare i propri token validi;
`klog`	consente di ottenere un nuovo *token*;
`unlog`	distrugge un token AFS;

`fs listquota` (short: `fs lq`)	Mostra le informazioni relative alla quota disco in AFS;
`fs quota`	Mostra la percentuale di quota utilizzata.

Gestione delle ACL:

I possibili diritti di accesso sono riassunti nella seguente tabella:

`l`	lookup	mostra l'elenco dei file in una directory;
`r`	read	consente la lettura del contenuto di un file;
`i`	insert	permette la creazione di nuovi file o directory;
`w`	write	autorizza a modificare un file;
`d`	delete	permette di cancellare file o directory;
`k`	lock	autorizza ad effettuare il lock dei file;
`a`	administer	consente di modificare le ACL.

Abbreviazioni:

all	tutti i diritti;
none	nessun diritto;
read	equivalente di **`rl`**
write	tutto tranne **`a`**

Comandi ACL:

`fs listacl` (short: `fs la`)	mostra le ACL di una determinata directory o della *current working directory* se nessuna directory e' specificata uso: **`fs listacl`** `[<directory>]`
`fs setacl` (short: `fs sa`)	definisce le ACL in una data directory, per un gruppo o un utente uso: **`fs setacl -dir`** `<directory>` **`-acl`** `<access list entries>` eg: **`fs setacl -dir`** *`privato`* **`-acl`** *`system:anyuser none`* (l'utente nega ogni diritto per la directory *privato* al gruppo *system:anyuser*) eg: **`fs setacl -dir`** *`nostra`* **`-acl`** *`pluto read`* (l'utente assegna il diritto di lettura per la directory *nostra* all'utente *pluto*)

`pts createg roup`	crea uno dei gruppi di proprieta' dell'utente a cui in seguito potranno essere assegnati i desiderati diritti di accesso a determinate directory uso: **`pts creategroup -name`** `<group name>` eg: **`pts creategroup -name`** *`pippo:amici`* (l'utente *pippo* crea il gruppo *amici*)
`pts delete`	rimuove uno dei gruppi di proprieta' dell'utente uso: **`pts delete -nameorid`** `<group name or id>` eg: **`pts delete -nameorid`** *`pippo:amici`* (l'utente *pippo* cancella il proprio gruppo *amici*)
`pts adduser`	aggiunge un utente (o host) ad un gruppo uso: **`pts adduser -user`** `<userid>` **`-group`** `<group name>` eg: **`pts adduser -user`** *`pluto`* **`-group`** *`pippo:amici`* (l'utente *pippo* aggiunge l'utente *pluto* al proprio gruppo *amici*)
`pts removeuser`	cancella un utente da un gruppo uso: **`pts removeuser -user`** `<userid>` **`-group`** `<group_name>` eg: **`pts removeuser -user`** *`pluto`* **`–group`** *`pippo:amici`* (l'utente *pippo* cancella l'utente *pluto* dal proprio gruppo *amici*)
`pts listowned`	mostra l'elenco dei gruppi che appartengono ad un determinato utente uso: **`pts listowned -nameorid`** `<userid>` eg: **`pts listowned -nameorid`** *`pippo`*
`pts membership`	se seguito dal nome di un gruppo, mostra l'elenco degli appartenenti a quel gruppo uso: **`pts membership`** `<group name>` eg: **`pts membership`** *`pippo:amici`* se seguito da una username, mostra l'elenco dei gruppi a cui quel determinato utente appartiene uso: **`pts membership`** `<username>` eg: **`pts membership`** *`pippo`*

E' disponibile un help in linea, richiamabile con

`fs help` o `pts help`

Per ulteriori informazioni

- *AFS User Guide*, documentazione ufficiale Transarc;
- Open AFS Documentation http://openafs.org/doc/index.htm.

last update: 11 luglio 2006 - d.a.