ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di Trieste

INFN/TC-97/17

giugno 27 1997

R. Gomezel e A. Maslennikov

Manuale di Installazione e Utilizzo del Programma ARC per la Cella AFS INFN.IT

SIS - Pubblicazioni
Laboratori Nazionali di Frascati

COP.

Manuale di installazione e utilizzo del programma ARC per la cella AFS INFN.IT

Versione 1.1

R.Gomezel(*) - A.Maslennikov(**)

27 giugno 1997

Sommario

Questo documento si propone di descrivere la procedura di installazione e le linee guida per l'utilizzo del programma ARC per la gestione decentralizzata dei server AFS di Sezione pertinenti alla cella INFN.IT.

(*)I.N.F.N. - Sezione di Trieste (**) CASPUR - Roma

Indice

1 Introduzione

ARC è l'acronimo di *Authenticated Remote Control*, programma sviluppato da Rainer Toebbicke (CERN/CN) che utilizza script di configurazione specifici che devono essere redatti dagli amministratori della cella di appartenenza.

Senza il programma ARC, la possibilità di gestire i server AFS che si trovano nelle diverse Sezioni dell'INFN era riservata esclusivamente a coloro che detengono i privilegi di amministratori dell'intera cella *infn.it* e che appartengono al gruppo *system:administrators*.

Al fine di permettere ai diversi gestori dei server di Sezione di poter operare come utenti privilegiati sul server di loro competenza, senza per questo consentire loro di operare su tutti gli altri server, evitando in questo modo la possibilità che vengano commessi, involontariamente, errori di gestione su parti dell'albero AFS i quali potrebbero compromettere la funzionalità dell'intera cella dell'INFN, è stata predisposta un'opportuna routine che permette ad un gestore di operare sul proprio server con tutti i privilegi normalmente posseduti soltanto dall'amministratore dell'intera cella, realizzando di fatto una gestione decentralizzata dei diversi volumi e di parti del sottoalbero AFS di pertinenza dell'INFN.

2 Il programma ARC

2.1 Quali sono le funzionalità previste dal programma ARC

Il programma ARC consente attualmente l'esecuzione dei seguenti comandi AFS sulle piattaforme Alpha (OSF/1 - DigitalUnix), AIX, HP (HP-UX), SUN (Solaris), SUN (OS) :

cruser <uid> <passwd> <quota> <lifetime> <userinfo> <section>

veruser <uid> [-verbose] - to verify a user

pwuser <uid> <new_password> - to reset user's password

lquser <uid> - to see the user's disk quota

squser <uid> <quota(KB)> - to set the user's disk quota

lltuser <uid> - to see user's token lifetime

sltuser <uid> <lifetime(hours)> - to set user's token lifetime

uinfo <uid> - to inspect the user's data

chuinfo <uid> <userinfo> - to update the user's data

rmuser <uid> - to remove a user

help [topic]

whoami

prelease <*projectname*> - to release volume project.<projectname>

vos suite: **addsite,backup,backupsys,create,dump,**
lock,move,release,remove,remsite,rename,
restore,syncserv,syncvldb,unlock,
unlockvldb,zap

fs suite : **mkmount,cleanacl,setquota,setvol,setacl,rmmount,copyacl**

bos suite : **restart,salvage,shutdown,start,stop**

Data la flessibilità della routine sarà possibile aggiungere ulteriori comandi qualora sorgerà la necessità in futuro.

2.2 Come si installa ARC sulla propria macchina

I prerequisiti per l'installazione di ARC su un host di Sezione sono i seguenti:

- deve appartenere ad una delle seguenti piattaforme: Alpha, HP,SUN o AIX
- deve essere un AFS client o server della cella *infn.it*

A questo punto la procedura di installazione è molto semplice; è sufficiente collegarsi alla macchina come root, in modo tale da eseguire i comandi come utente privilegiato.

Eseguire il seguente comando:

 # /afs/infn.it/system/usr/share/sue/feature/arc/install.arc <*ARC Server*>

attualmente l'host da specificare come ARC Server è **kiwi.caspur.it**, ma nel prossimo futuro verrà utilizzato come server ARC una macchina del CNAF.

Se l'installazione ha avuto successo comparirà il seguente messaggio prima del prompt di sistema:

INFN arc client for host <nome host> successfully configured...

A questo punto la macchina disporrà della routine ARC, la quale consentirà al gestore del server di Sezione di eseguire i comandi indicati nel paragrafo precedente.

Il nome del gestore dovrà essere inserito in un opportuno database di autorizzazione da parte di uno degli amministratori dell'intera cella *infn.it*.

2.3 Come si utilizza ARC

Come si è già anticipato nel paragrafo precedente, per poter eseguire i comandi privilegiati sul proprio server è necessario essere stati inseriti all'interno del database di autorizzazione di ARC che consiste in un file il cui accesso e' consentito soltanto all'amministratore della cella infn.it. Qualora tale nome non compaia all'interno del file gli unici comandi che si possono eseguire sono, oltre a quelli non privilegiati , anche i comandi arc *help* e *whoami*.

Per eseguire i comandi che non necessitano di particolari privilegi non occorre utilizzare ARC, mentre per i comandi help e whoami si utilizzerà il seguente comando:

 # /afs/usr/local/etc/arc -P -p -h <*ARC Server*> **<help** *or* **whoami>**

dove per ARC Server si deve specificare sempre **kiwi.caspur.it**.

Il nome dell'ARC Server successivo al flag *-h* è richiesto ogniqualvolta si esegue un comando per mezzo di ARC, perchè ARC utilizza per la cella infn.it un processo di quell'host al fine di accordare gli opportuni privilegi al gestore del server di Sezione.

Qualora il nome del gestore sia stato inserito nel database di autorizzazione di ARC, egli potrà eseguire tutti i comandi previsti sui volumi gestiti dal server locale ,tutto il sottoalbero AFS contenuto all'interno del proprio server e i processi del proprio server, mentre gli saranno negate le stesse operazioni su parti del sottoalbero AFS o volumi che non sono sotto la sua responsabilità.

Questo accorda al gestore la libertà di gestire il suo spazio AFS, ma non gli consente di compromettere per errore la funzionalità operativa degli altri server o della cella *infn.it*; nonostante cio', il gestore deve prestare molta attenzione alle operazioni che esegue anche sul proprio server, perche' comunque queste azioni possono produrre ripercussioni indesiderate sulle funzionalità complessive della cella, data la natura distribuita del file system AFS.

2.4 I comandi privilegiati messi a disposizione da ARC

I comandi privilegiati che si possono eseguire attraverso il filtro di ARC sono quelli già elencati nel *paragrafo 1.1*; per maggiori dettagli si rimanda al *Command Reference Manual* di AFS.

Innanzi tutto, si deve premettere che ciascuno dei comandi privilegiati AFS previsti all'interno di ARC devono essere preceduti dalla chiamata alla routine ARC come già anticipato nel *paragrafo 1.3* per i comandi *help* e *whoami*; tale comando è stato definito, per tutte le architetture previste, sotto la directory afs **/afs/usr/local/etc.**

Dopo aver installato l'ARC client su una macchina di Sezione e dopo che il nome del gestore del server di Sezione è stato inserito nel database di autenticazione, il gestore deve

- collegarsi all'host che funge da ARC client con login-AFS come utente gestore;
- controllare che nel PATH siano presenti */usr/afsws/bin, /usr/afsws/etc, /afs/usr/local/bin, /afs/usr/local/etc*
- eseguire *klog.krb* con la medesima password.

Per poter eseguire i comandi indicati sarà pertanto necessario premettere loro il comando **arc** specificando i flag **-p** e **-h**.

Il flag **-p** non è opzionale, pena l'impossibilita' di eseguire il comando, perchè esso attiva una comunicazione che utilizza Kerberos, al fine di garantire la sicurezza durante l'esecuzione del comando privilegiato.

Il flag **-h** va seguito dal nome del server ARC che si incarica di effettuare le opportune verifiche per quel che riguarda l'autenticazione del gestore sul server di Sezione come specificato nel database di autenticazione; nel caso della cella *infn.it* il server da indicare è attualmente ***kiwi.caspur.it***.

Di seguito va specificato il comando che si vuole eseguire con i relativi campi specifici.

Esempio:

 # arc -p -h *<ARC Server>* *<comando afs>*

I comandi afs previsti per la gestione dei server e dei processi relativi sono **fs,vos e bos**, mentre per la gestione degli utenti sotto afs sono stati definiti i seguenti comandi:

- **cruser** - consente la creazione di un *account* sotto afs; i sei parametri, da specificare nell'ordine, sono i seguenti:
  - *username* : nome dell'utente che si vuole creare e che deve essere unico all'interno della cella INFN.IT; il nome può essere composto al massimo da 8 caratteri (lettere o cifre), il primo carattere non deve essere un carattere numerico;
  - *password*: la password deve essere composta da almeno 8 caratteri (lettere dell'alfabeto o cifre)
  - *quota*: valore in KB della quota da assegnare al volume dell'utente;
  - *token lifetime*: tempo di vita del token in ore;
  - *informazioni sull'utente*: le informazioni relative all'utente che vanno definite all'interno del database degli utenti della cella; la sintassi del formato è la seguente:

    Nome+Cognome+Telefono+Indirizzo E-mail+

    i campi devono essere separati dal carattere "+", mentre gli eventuali spazi bianchi vanno indicati con il carattere di sottolineatura (underscore).
    Esempio: Vincenzo_Di_Martino.
  - *sezione* : serve ad indicare la sezione INFN cui l'utente fa riferimento (prefisso)
- **veruser** <*uid*> - permette di verificare l'esistenza dell'utente specificato;
- **pwuser** <*uid*> <*new_password*> - consente di modificare la password di un utente gia' creato;
- **lquser** <*uid*> - visualizza la quota assegnata al volume dell'utente indicato;
- **squser** <*uid*> <*quota(KB)*> - consente di modificare la quota di un utente;
- **lltuser** <*uid*> - visualizza il tempo di vita del token di un determinato utente;
- **sltuser** <*uid*> <*lifetime(hours)*> - consente di modificare il tempo di vita del token asseganto ad un utente;
- **uinfo** <*uid*> - visualizza le informazioni relative all'account di un determinato utente;
- **chuinfo** <*uid*> <*userinfo*> - rende possibile la modifica delle informazioni relative ad un utente specifico;
- **rmuser** <*uid*> - comando per rimuovere l'account di un utente.

Comunque per poter visualizzare tutti i comandi disponibili si può utilizzare il comando

 # arc -p -h <*ARC Server*> **help**

mentre per poter vedere la sintassi corretta da utilizzare e gli argomenti dei comandi che devono essere necessariamente indicati affinche' venga autorizzata la loro esecuzione si può far riferimento al comando

 # arc -p -h <*ARC Server*> **help** <*comando*>

oppure all'*Appendice* ; qualora un argomento non venga specificato, verrà notificata la sua mancanza mediante un opportuna segnalazione d'errore; inoltre devono essere specificati cosí come indicati nell'elenco e non abbreviati, per motivi di sicurezza legati al parsing di ARC.

È comunque sempre possibile definire degli script di shell che prevedano l'uso di abbreviazioni e consentano di non dover premettere il richiamo ad arc prima di ogni richiesta di esecuzione di comando privilegiato.

3 Appendice

- **vos addsite -server** <*nome macchina*> **-partition** <*nome partizione*> **-id** <*nome volume o ID*>
- **vos backup -id** <*nome volume o ID*>
- **vos backupsys**
- **vos create -server** <*nome macchina*> **-partition** <*nome partizione*> **-name** <*nome volume*>
- **vos dump -id** <*nome volume o ID*>
- **vos lock -id** <*nome volume o ID*>
- **vos move -id** <*nome volume o ID*> **-fromserver** <*nome macchina*> **-frompartition** <*nome partizione*> **-toserver** <*nome macchina*> **-topartition** <*nome partizione*>
- **vos release -id** <*nome volume o ID*>
- **vos remove -server** <*nome macchina*> **-partition** <*nome partizione*> **-id** <*nome volume o ID*>
- **vos remsite -server** <*nome macchina*> **-partition** <*nome partizione*> **-id** <*nome volume o ID*>
- **vos rename -oldname** <*nome volume vecchio*> **-newname** <*nome volume nuovo*>
- **vos restore -server** <*nome macchina*> **-partition** <*nome partizione*> **-name** <*nome del volume*>
- **vos syncserv -server** <*nome macchina*>
- **vos syncvldb -server** <*nome macchina*>
- **vos unlock -id** <*nome volume o ID*>
- **vos unlockvldb -server** <*nome macchina*>
- **vos zap -server** <*nome macchina*> **-partition** <*nome partizione*> **-id** <*nome volume o ID*>
- **fs mkmount -dir** <*nome directory*> **-vol** <*nome volume*>
- **fs cleanacl -path** <*dir/file path*>
- **fs setquota -path** <*dir/file path*>
- **fs setvol -path** <*dir/file path*>
- **fs setacl -dir** <*nome directory*> **-acl** <*access list entry*>
- **fs rmmount -dir** <*nome directory*>
- **fs copyacl -fromdir** <*nome directory*> **-todir** <*nome directory*>

- **bos restart -server** <*nome server*>
- **bos salvage -server** <*nome server*>
- **bos shutdown -server** <*nome server*>
- **bos start -server** <*nome server*>
- **bos stop -server** <*nome server*>

inoltre sono stati previsti i seguenti comandi:

- **help** : che visualizza l'elenco dei comandi disponibili via arc
- **whoami :** simile al comando whoami Unix per l'identificazione dell'utente sotto AFS
- **prelease** <nome progetto> : per l'esecuzione del vos release su volumi di progetto (vedi kloe e atlas)
- **cruser** <uid> <passwd> <quota> <lifetime> <userinfo> <section>
- **veruser** <uid> **[-verbose]**
- **pwuser** <uid> <new_password>
- **lquser** <uid>
- **squser** <uid> <quota(KB)>
- **lltuser** <uid>
- **sltuser** <uid> <lifetime(hours)>
- **uinfo** <uid>
- **chuinfo** <uid> <userinfo>
- **rmuser** <uid>