Migrazione Da Kaserver a KDC Kerberos 5 in Una Cella AFS

- Interoperabilità tra Unix, AFS e Windows 2000
- GUI Netuser per la gestione degli utenti Unix e Windows

di

Fulvio Ricciardi

e

Enrico M. V. Fasanelli

INFN LECCE

I vantaggi di Kerberos 5 rispetto al Kaserver

- Interoperabilità tra mondo UNIX, WINDOWS 2000 e AFS
  - Semplicità amministrativa: infatti ogni utente ha un unico principale di autenticazione valido sia per UNIX che per WINDOWS
  - L'utente può cambiare la sua password sia da UNIX con il comando kpasswd che da WINDOWS con la pressione della combinazione di tasti CTRL+ALT+DEL
  - Possibilità del Client AFS per Windows di ottenere il token al momento del logon senza preoccuparsi di dover impostare la password Windows uguale a quella AFS

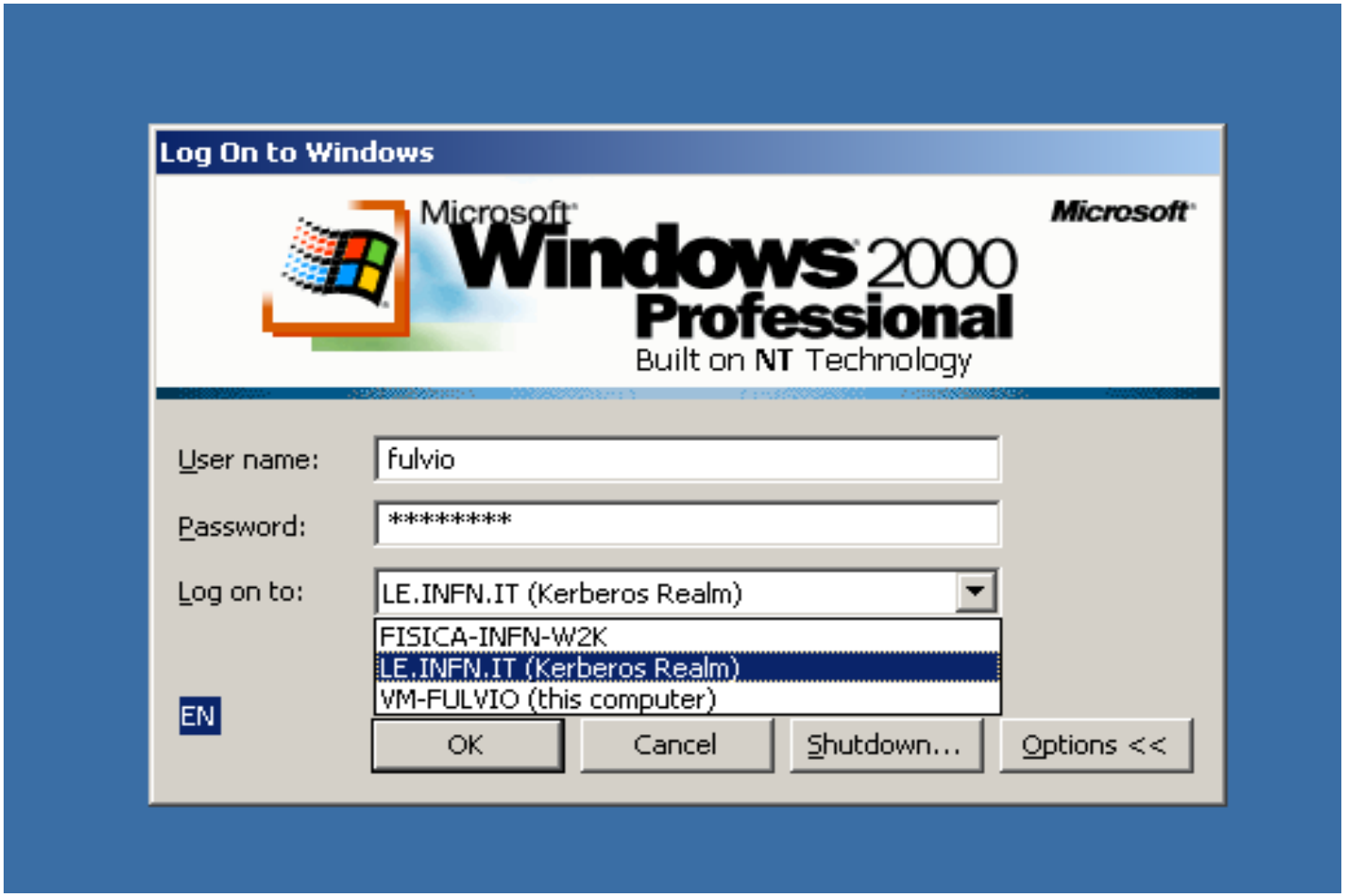
- Possibilità di impiego di servizi kerberos 5 (ssh, rsh, telnet, ftp, autenticazione del Router Cisco, ecc.)

SSH Single Sign-on con Kerberos 5

```
pluto:fulvio > kinit -f fulvio
Password for fulvio@LE.INFN.IT:
pluto:fulvio >
pluto:fulvio > klist
Ticket cache: FILE:/tmp/krb5cc_7013_65gCzp
Default principal: fulvio@LE.INFN.IT
Valid starting     Expires            Service principal
05/03/02 14:16:20  05/04/02 00:16:20  krbtgt/LE.INFN.IT@LE.INFN.IT
pluto:fulvio >
pluto:fulvio > ssh pocahontas
Last login: Fri May  3 14:15:33 2002 from pluto.le.infn.it
Fri May  3 14:16:47 MEST 2002
pocahontas:fulvio >
pocahontas:fulvio > ssh sirio  uptime
  2:38pm  up 38 days, 1:58,   1 user,   load average:   0.00,  0.00,  0.00
sirio:fulvio >
```

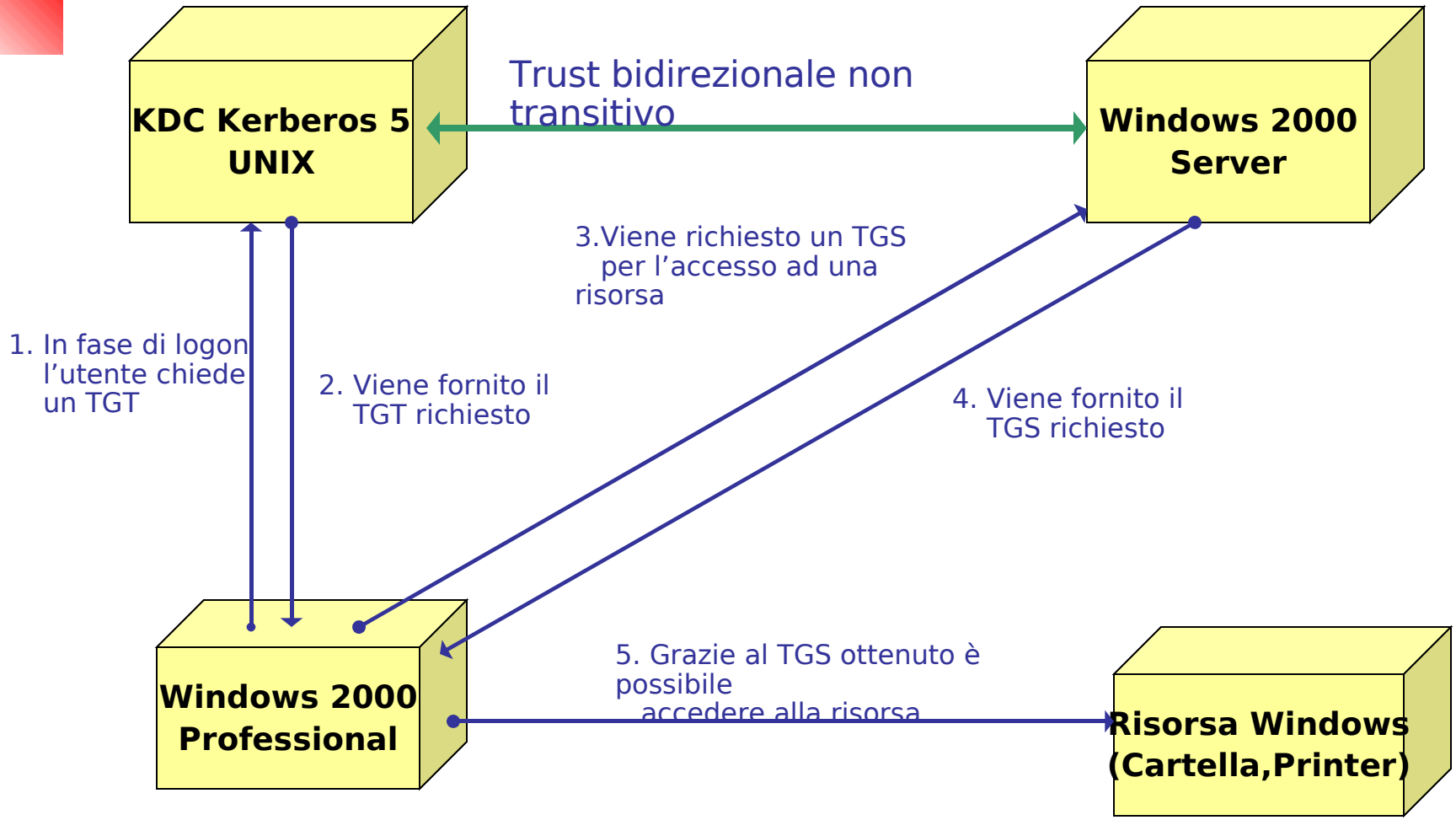
Come si può notare, una volta ottenuto il ticket, è possibile fare login con SSH senza dover ridigitare nuovamente la password.

Logon in Windows 2000 con Kerberos 5 Unix



Kpasswd in ambiente Windows 2000

Funzionamento del trust tra KDC Unix e KDC Windows



Due strade percorribili (Soluzione A)

A. Il KDC distribuisce solo tickets Kerberos 5

Vantaggi:

- Maggiore sicurezza intrinseca al protocollo Kerberos 5

Svantaggi:

- E' necessaria la sostituzione del metodo di autenticazione in tutti i client UNIX
- Non è più possibile usare il comando klog di AFS

  klog fulvio => kinit fulvio (per ottenere il TGT)

  afslog (per ottenere il token AFS)
- Gli utenti autenticati in una cella esterna non potendo usare il comando klog fulvio –cell le.infn.it se non dispongono dei comandi kinit e afslog non possono autenticarsi in le.infn.it

Due strade percorribili (Soluzione B)

A. Il KDC distribuisce anche tickets Kerberos 4 e tokens AFS oltre ovviamente a tickets Kerberos 5

Vantaggi:

- Il metodo di autenticazione nelle macchine UNIX può rimanere invariato poiché continuano ad essere distribuiti i tokens AFS
- Gli utenti UNIX non si accorgono del cambiamento poiché possono continuare ad usare il klog per ottenere un token AFS

Svantaggi:

- Una minore sicurezza dovuta all'utilizzo dei protocolli Kerberos 4 e RX del KASERVER di AFS (ma comunque pari alla sicurezza che si ha nell'utilizzo del Kaserver)
- Configurazione del KDC più complicata

La soluzione che abbiamo preferito a Lecce è la B

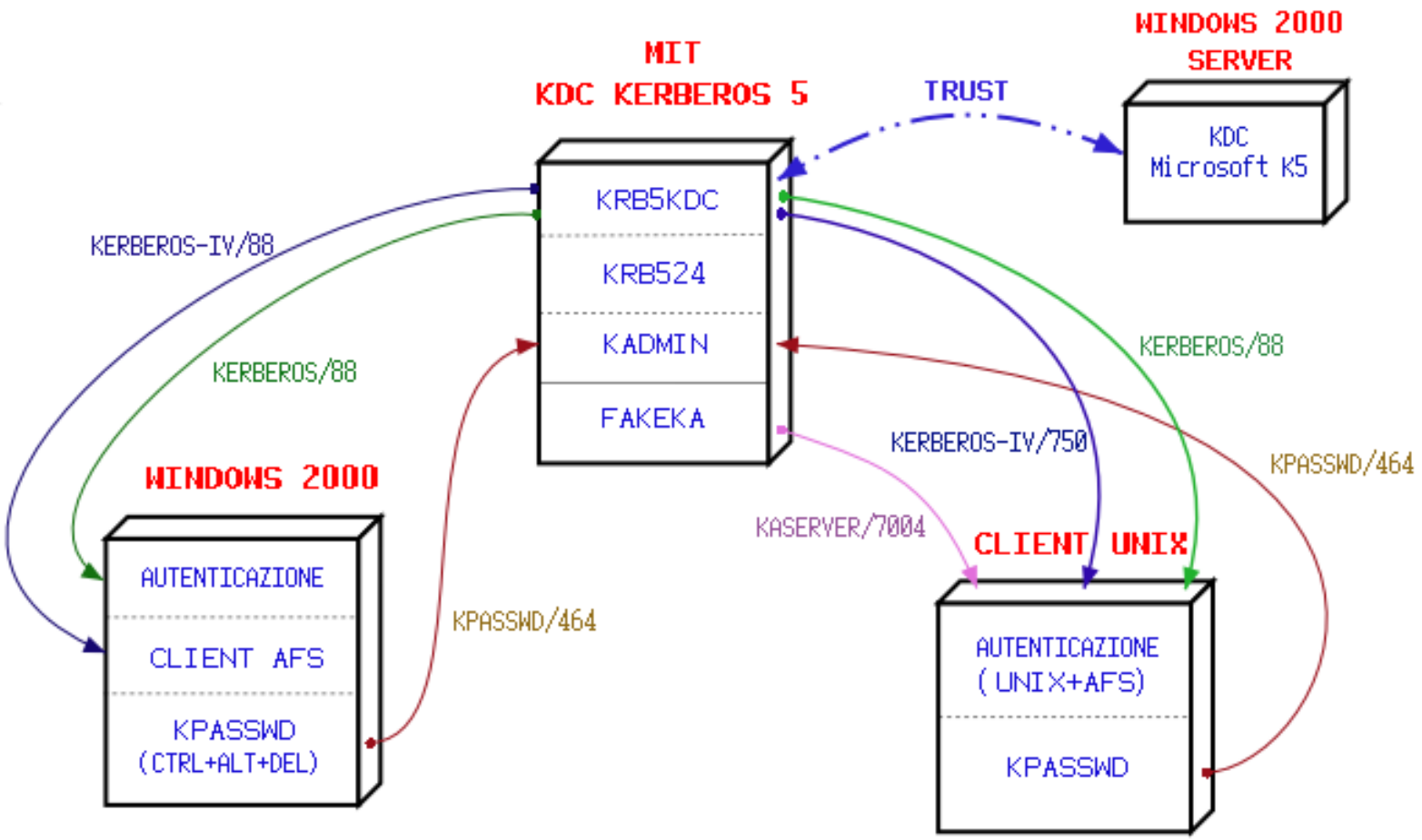
- Cioè continuare a supportare il protocollo di autenticazione del Kaserver

Quale implementazione di Kerberos 5?

- A questo punto bisogna decidere quale implementazione di Kerberos 5 adottare:
  - L'implementazione di Kerberos 5 di MIT con l'aggiunta di fakeka (fake Kaserver) appartenente al Migration Kit di Ken Hornstein
  - L'implementazione di Kerberos 5 di Heimdal che può distribuire in maniera nativa tokens AFS senza l'aggiunta di componenti esterni
  - Combinare entrambe le implementazioni in una struttura MASTER/SLAVE, ottenendo così, i vantaggi dell'una e dell'altra implementazione

Nota: scartiamo a priori l'implementazione Microsoft del Kerberos 5 presente in Windows 2000 Server poiché oltre a non essere perfettamente conforme al protocollo, potrà difficilmente fornire ticket Kerberos 4 e ancor meno tokens AFS

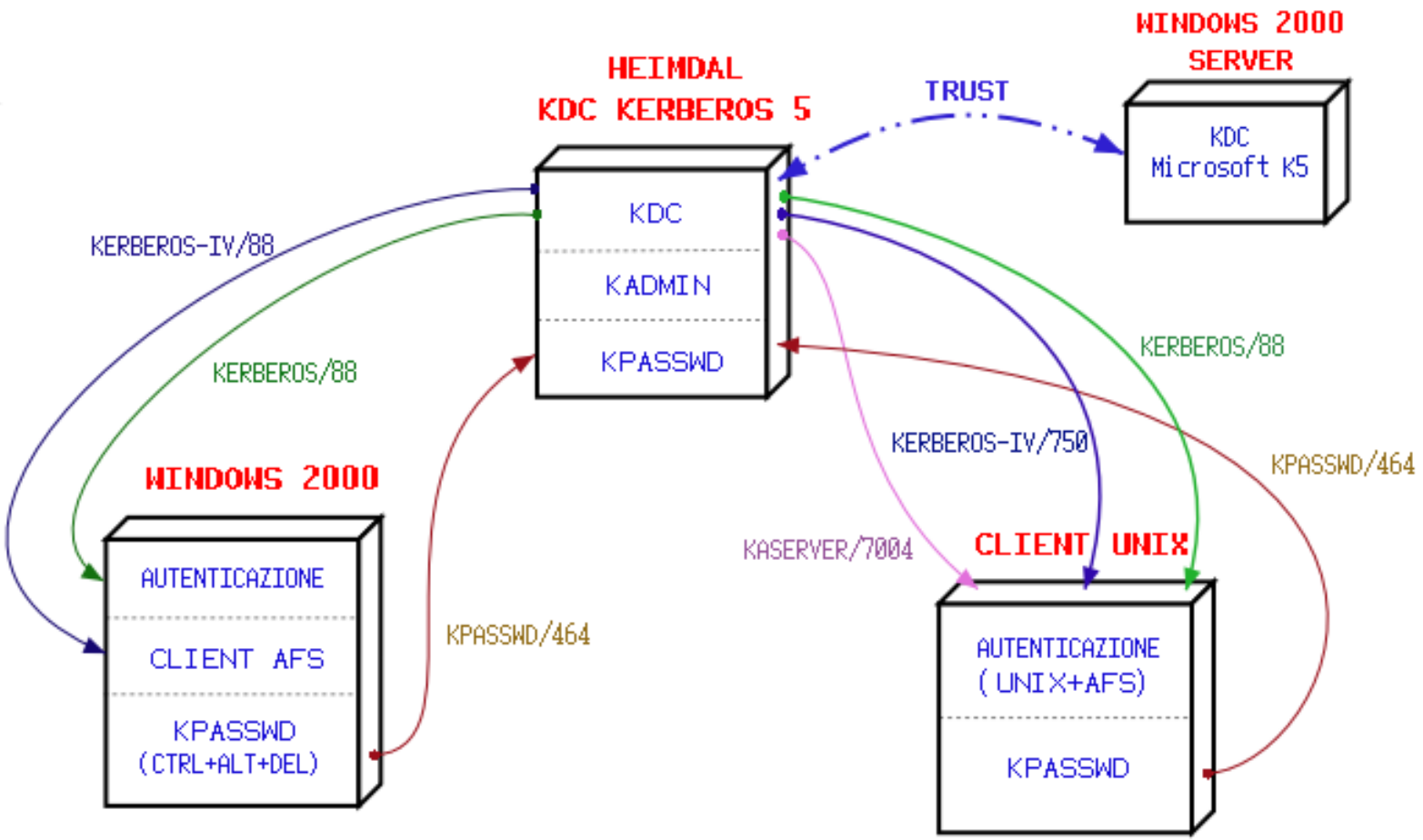
MIT Kerberos 5 (Interoperabilità)



Vantaggi e svantaggi del MIT Kerberos 5

- Vantaggi:
  - Completa interoperabilità con Windows 2000. Tale interoperabilità e ben documentata da Microsoft
  - http://www.microsoft.com/windows2000/techinfo/planning/security/kerbsteps.asp
- Svantaggi:
  - Un probabile bug nella parte di codice del KDC riguardante la distribuzione di tickets V4 impedisce al Client AFS per Windows di funzionare correttamente: infatti se il timelife del ticket supera le 12 ore allora il ticket scadrebbe nell'anno 1601!!! Ovviamente tale ticket è inutilizzabile in quanto già scaduto prima di essere emesso.
  - Necessità nella fase di setup del KDC di usare l'utility afs2k5db del Migration Kit per convertire le chiavi contenute nel database del Kaserver se si vogliono conservare le password degli utenti
  - Alcune vecchie versioni di AFS per UNIX non si autenticano con il fakeka
  - Fakeka e afs2k5db sono comunque componenti esterni al pacchetto di MIT scritti per la versione 1.0.6 e spesso

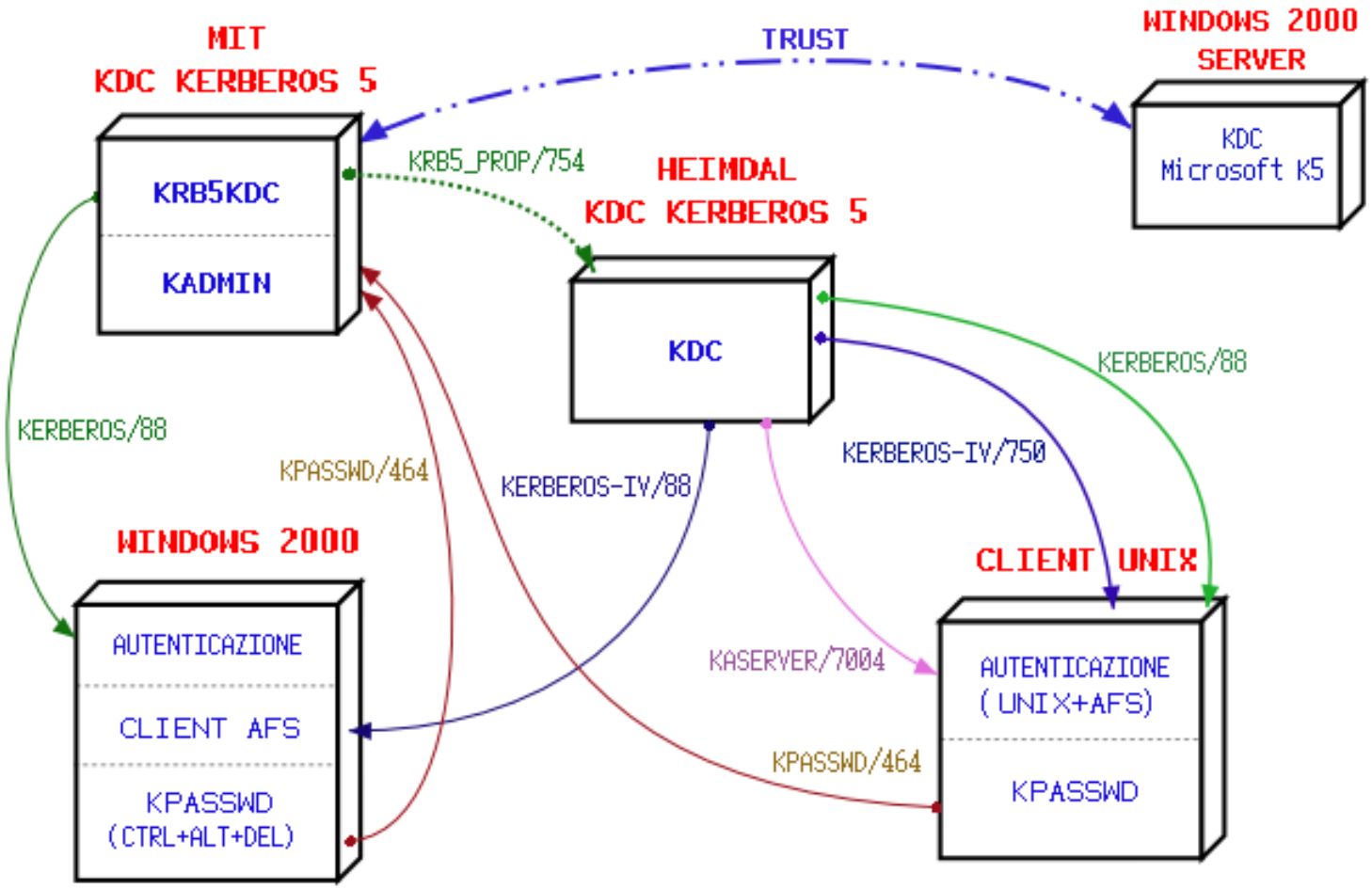
HEIMDAL Kerberos 5 (Interoperabilità)



Vantaggi e svantaggi di Heimdal Kerberos 5

- Vantaggi:
  - Il KDC dell'implementazione di Heimdal contiene già in maniera nativa il codice per l'emulazione del Kaserver
  - In fase di setup del KDC la migrazione delle chiavi presenti nel database del Kaserver avviene con strumenti presenti nell'implementazione:
    - hprop –source=kaserver –d /usr/afs/db/kaserver.DB0 -n | hpropd -n
  - Nessun problema di autenticazione sia che si tratti di vecchie versioni di AFS per UNIX che del client AFS per Windows
- Svantaggi:
  - L'interoperabilità con Windows 2000 non è direttamente documentata da Microsoft e dalla nostra esperienza risulta non completamente attuabile. Infatti, benché gli utenti vengano autenticati in Windows 2000, poi, in realtà, non riescono ad accedere alle risorse quali cartelle condivise, stampanti e quindi a mappare le unità AFS.

Kerberos 5 MIT e HEIMDAL in una struttura MASTER/SLAVE



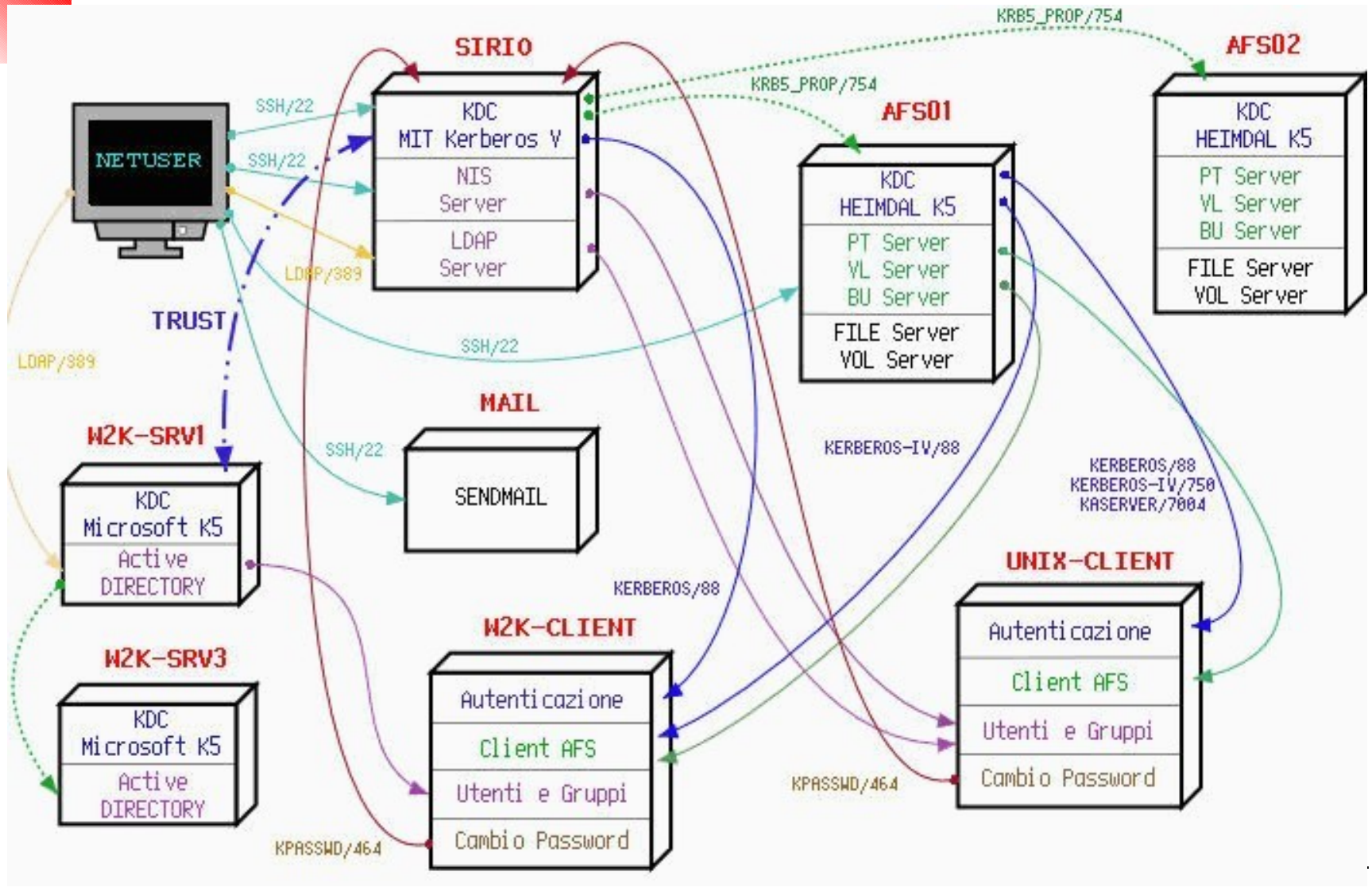
Vantaggi e svantaggi dell'impiego combinato dell'implementazione MIT e HEIMDAL

- Vantaggi:
  - Tutti i vantaggi delle due soluzioni precedenti, cioè:
    - Perfetta interoperabilità tra mondo UNIX,AFS e WINDOWS 2000
    - Kaserver implementato in maniera nativa nel KDC
    - Autenticazione funzionante su qualsiasi Client AFS sia UNIX che WINDOWS
- Svantaggi:
  - Configurazione più complicata
  - Poiché il KDC master è quello di MIT, mentre lo slave è quello di HEIMDAL, per precaricare le chiavi presenti nel database del Kaserver è necessario l'uso dell'utility afs2k5db del Migration Kit

L’implementazione che abbiamo scelto a Lecce è la terza

- Cioè, combinare insieme l’implementazione di MIT e di HEIMDAL in una struttura Master/Slave, per sfruttare i vantaggi dell’una e dell’altra implementazione.

Autenticazione e Protezione nella Cella le.infn.it



Descrizione dei sistemi

- **sirio.le.infn.it** (cname KerberosMIT, nis01) (Red Hat 7.2)
  - È un biprocessore 1U P!!!1000Mhz con 1GB di RAM ECC e 2 HD 60GB ATA100 in RAID 1. La sua funzione principale è di KDC (MIT) Master, ma svolge anche la funzione di NIS master, di server LDAP, di server SYSLOG e di server LPD
- **afs01.le.infn.it** (cname nis02) (Red Hat 7.2)
  - È un biprocessore 4U P!!!1000Mhz con 1GB di RAM ECC e 8 HD 60 GB ATA100 in RAID 5. Può ospitare fino a 16 dischi EIDE distribuiti su due controller 3ware Escalade 7850. La sua funzione principale è di file server e authentication server per AFS. Su di esso il KASERVER è stato sostituito con il KDC Heimdal.
- **afs02.le.infn.it** (cname nis03) (Red Hat 7.2)
  - Come afs01
- **w2k-srv1.le.infn.it** (W2K Server)
  - È un biprocessore 1U P!!!1000Mhz con 1GB di RAM ECC e 2 HD 60GB ATA100 in RAID 1. E' uno dei due Windows 2000 Server del dominio w2k.le.infn.it
- **w2k-srv3.le.infn.it** (W2K

Realizzazione del sistema di autenticazione Kerberos 5 MIT/HEIMDAL

- Nelle pagine che seguono viene esposta la procedura per la realizzazione del sistema di autenticazione Kerberos 5 MIT/HEIMDAL.
- Tale sistema, in produzione nella cella AFS le.infn.it di Lecce da Settembre 2001, è stato realizzato dapprima su architetture ALPHA con sistema Digital Unix 4.0f ed ora definitivamente migrato su piattaforme INTEL con sistema Linux Red Hat 7.2
- I test che consistono nell'uso quotidiano del sistema comprendono:
  - 48 sistemi Linux Red Hat (comprese le macchine di servizio)
  - 7 sistemi Digital Unix 4.0
  - 32 sistemi Windows 2000 Professional sotto il dominio w2k.le.infn.it
  - 1 server IMAP su Digital 4.0f che dai log dei KDC risulta quello che più di tutti sfrutta l'autenticazione a causa degli automatismi dei MUA che possono controllare la posta anche una volta al minuto

Versione del software utilizzato

- Sistema operativo:
  - Red Hat 7.2
- MIT Kerberos 5:
  - 1.2.2 installato direttamente dagli rpm
    - krb5-server-1.2.2-13.i386.rpm
    - krb5-workstation-1.2.2-13.i386.rpm
    - krb5-libs-1.2.2-13.i386.rpm
- HEIMDAL Kerberos 5:
  - 0.4b i cui sorgenti sono disponibili all'URL ftp://ftp.pdc.kth.se/pub/heimdal/src/heimdal-0.4b.tar.gz
- Kerberos 4 (necessario per compilare Heimdal Kerberos 5):
  - 1.0.9 i cui sorgenti sono disponibili all'URL ftp://ftp.pdc.kth.se/pub/krb/src/krb4-1.0.9.tar.gz
- Migration Kit di Ken Hornstein:
  - 1.3 i cui sorgenti sono disponibili all'URL ftp://ftp.cmf.nrl.navy.mil/pub/kerberos5/afs-krb5-1.3.tar.gz
- OpenAFS:
  - 1.2.2a i cui sorgenti sono disponibili all'URL
  - http://www.openafs.org/openafs/1.2.2a/openafs-1.2.2a-src.tar.gz

Installare MIT kerberos 5 su SIRIO

Può essere installato direttamente dai pacchetti rpm di Red Hat:

```
[root@sirio]# rpm –ivh krb5-libs-1.2.2-13.i386.rpm
[root@sirio]# rpm –ivh krb5-workstation-1.2.2-13.i386.rpm
[root@sirio]# rpm –ivh krb5-server-1.2.2-13.i386.rpm
```

Configurare /etc/krb5.conf di MIT Kerberos 5 su SIRIO

```
[logging]
        default = FILE:/var/kerberos/krb5kdc/kdc.log
         kdc = FILE:/var/kerberos/krb5kdc/kdc.log
        admin_server = FILE:/var/kerberos/krb5kdc/kdc.log
[libdefaults]
         ticket_lifetime = 24000
        default_realm = LE.INFN.IT
 [realms]
        LE.INFN.IT= {
                kdc = afs02.le.infn.it:88
                admin_server = sirio.le.infn.it:749
                default_domain = le.infn.it
        }
[domain_realm]
         .le.infn.it= LE.INFN.IT
         le.infn.it= LE.INFN.IT
[kdc]
        profile = /var/kerberos/krb5kdc/kdc.conf
[pam]
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
         forwardable = true
         krb4_convert = false
```

Configurare /var/kerberos/krb5kdc/kdc.conf di MIT Kerberos 5 su SIRIO

```
[kdcdefaults]
 acl_file = /var/kerberos/krb5kdc/kadm5.acl
 dict_file = /usr/share/dict/words
 admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab

[realms]
 LE.INFN.IT = {
  master_key_type = des-cbc-crc
  supported_enctypes = des-cbc-crc:normal des-cbc-crc:v4 des-cbc-crc:afs3
  max_life = "30 day"
 }
```

Molto importante in questo file è la voce supported_enctypes. Questa indica al kadmin (al demone e non solo all'interfaccia di amministrazione) quali chiavi generare quando viene aggiunto un nuovo utente o quando viene cambiata la password. La prima chiave (des-cbc-crc:normal) è essenziale per Windows 2000, mentre l'ultima (des-cbc-crc:afs3) permette l'autenticazione AFS. Dopo l'importazione delle chiavi dal Kaserver, ovviamente, è presente solo la chiave afs3 e perciò i vecchi utenti per poter effettuare il logon in Windows devono cambiarsi

Creare il Regno Kerberos LE.INFN.IT e importare le chiavi dal Kaserver

[root@sirio]# kdb5_util create LE.INFN.IT –s

In questa fase viene richiesta la Master Key che serve a crittografare il database di Kerberos. L'hash di tale
chiave viene memorizzato nel file /var/kerberos/krb5kdc/.k5.LE.INFN.IT. Aggiungiamo ora le seguenti chiavi di
servizio che servono ad autenticare l'amministrazione remota e il cambio di password:

[root@sirio]# kadmin.local –q "ktadd –k /var/kerberos/krb5kdc/kadm5.keytab kadmin/admin"
[root@sirio]# kadmin.local –q "ktadd –k /var/kerberos/krb5kdc/kadm5.keytab kadmin/changepw"

Supposto ora che il database del kaserver /usr/afs/db/kaserver.DB0 sia stato copiato nella directory /tmp di
SIRIO è possibile effettuare la migrazione come segue:

[root@sirio]# afs2k5db -l 30d /tmp/kaserver.DB0 > /tmp/kaserver.mit
[root@sirio]# kdb5_util load -update –verbose /tmp/kaserver.mit

A questo punto il database di MIT Kerberos 5 è popolato con i principali degli utenti presenti nel Kaserver.
Ovviamente vi è anche la chiave afs@LE.INFN.IT che è il ticket di servizio (o token AFS) per l'accesso ad AFS.
Aggiungiamo ancora i seguenti 3 principali di autenticazione che serviranno ad autenticare il servizio di replica
che è esso stesso un servizio kerberizzato:

[root@sirio]# kadmin.local -q "addprinc -randkey kadmin/hprop"

Avviare i servizi KRB5KDC e KADMIN di MIT

La distribuzione di Red Hat, nei pacchetti RPM di Kerberos 5, contiene già gli script per lo
start/stop/restart dei servizi Kerberos. Per attivare il KDC MIT sono perciò sufficienti i comandi:

```
[root@sirio]# /etc/init.d/krb5kdc start
[root@sirio]# /etc/init.d/kadmin start
```

e per automatizzare la partenza durante il boot:

```
[root@sirio]# chkconfig krb5kdc on
[root@sirio]# chkconfig kadmin on
```

E’ da notare che MIT Kerberos 5 ha anche il servizio KRB524 (porta 4444). Lo scopo di questo
demone è quello di permettere, conformemente allo stile Single sign-on, ad un utente che ha
già un ticket v5, di ottenerne uno v4 senza dover ridigitare la password. Noi non facciamo
partire questo demone su SIRIO perché tanto questa questa funzione è svolta dal

Installare HEIMDAL kerberos 5 su AFS01

Per installare Heimdal Kerberos 5 è necessario compilarne il codice sorgente poiché nella
distribuzione di Red Hat non vengono forniti gli RPM di questo pacchetto. I sorgenti possono
essere prelevati all'URL:

ftp://ftp.pdc.kth.se/pub/heimdal/src/heimdal-0.4b.tar.gz

Se si sceglie, come nel nostro caso, di fornire anche ticket K4 e tokens AFS, è necessario
compilare anche Kerberos 4 prelevabile all'URL:

ftp://ftp.pdc.kth.se/pub/krb/src/krb4-1.0.9.tar.gz

A questo punto entrati nella directory dei sorgenti di Kerberos 4 dare i comandi:

```
[root@afs01]# ./configure && make && make install
```

E in maniera simile nella directory dei sorgenti di Heimdal Kerberos 5:

```
[root@afs01]# ./configure && make && make install
```

A questo punto Heimdal Kerberos 5 è installato sotto la directory /usr/heimdal

Configurare /etc/krb5.conf di Heimdal Kerberos 5 su AFS01

```
[libdefaults]
        default_realm = LE.INFN.IT
       clockskew = 300
       v4_instance_resolve = false
[realms]
       LE.INFN.IT = {
                kdc = afs02.le.infn.it
                admin_server = sirio.le.infn.it
       }
       default_domain = le.infn.it
[domain_realm]
       .le.infn.it = LE.INFN.IT
       le.infn.it = LE.INFN.IT
[kdc]
       enable-kaserver = true
       enable-kerberos4 = true
        enable-524 = true
       v4-realm = LE.INFN.IT
[kadmin]
       default_keys = v5 v4 des-cbc-crc:afs3-salt:le.infn.it
[logging]
       kdc = FILE:/var/heimdal/kdc.log
       kdc = SYSLOG:INFO
       default = SYSLOG:INFO:USER
```

Creare il database del KDC HEIMDAL

Prima di poter creare il database per il KDC Heimdal è necessario copiare lo stash file, cioè il file
contenente la Master Key, da SIRIO su AFS01:

```
[root@afs01]# scp sirio:/var/kerberos/krb5kdc/.k5.LE.INFN.IT
    /var/heimdal/m-key
```

quindi è possibile creare il database:

```
[root@afs01]# /usr/heimdal/sbin/kadmin  -l  init  LE.INFN.IT
```

Infine è necessario popolarlo con le chiavi presenti nel database del KDC MIT presente su
SIRIO:

```
[root@sirio]# /usr/kerberos/sbin/kdb5_util  dump  -b7  >  /tmp/mit.dump
[root@afs01]# scp sirio:/tmp/mit.dump  /tmp
[root@afs01]# cd /usr/heimdal/libexec
[root@afs01]# ./hprop  --source=mit-dump  -d /tmp/mit.dump  -n  |
    ./hpropd  -n
```

Nota: Popolare il database in questa fase può sembrare un'operazione superflua, visto che comunque il KDC Heimdal presente su AFS01 è uno slave di quello MIT presente su SIRIO. D'altra parte però, ciò è necessario, in quanto il meccanismo di replica Master/Slave è esso stesso un servizio kerberizzato che per poter funzionare deve chiedere il ticket di servizio hprop/afs01.le.infn.it al KDC di AFS01 stesso. Ne deriva da ciò che le operazioni di replica automatica funzionano solo a regime e non nella fase di setup del KDC quando il database è

Predisporre il push delle repliche su SIRIO

La replica del database da SIRIO (master) verso AFS01 e AFS02 (slave) deve avvenire solo quando si verifica
una modifica del file /var/kerberos/krb5kdc/principal contenente appunto il database. Tali repliche avvengono
quindi in corrispondenza del cambio di password da parte di un utente ovvero quando un amministratore
effettua una modifica con kadmin. Uno script utile ad ottenere tale risultato è il seguente:

```
#!/bin/sh
TMPFILE=/tmp/kdc.dump
X="`sum /var/kerberos/krb5kdc/principal`"
while true ; do
   if [ "$X" != "`sum /var/kerberos/krb5kdc/principal`" ] ; then
      X="`sum /var/kerberos/krb5kdc/principal`“
      /usr/kerberos/sbin/kdb5_util dump -b7 > $TMPFILE
      /usr/heimdal/libexec/hprop --source=mit-dump -d $TMPFILE  afs01 afs02
      logger "KERBEROS 5 database pushed"
      rm -f $TMPFILE
  fi
  sleep 1
done
```

Nota: Sperimentalmente abbiamo verificato, che con un database contenente circa 300 principali (quale quello di Lecce), il carico di sistema dovuto al calcolo del checksum una volta al secondo è del tutto trascurabile. Un altro approccio potrebbe essere quello di schedulare la replica in un cronjob, indipendentemente dal fatto che sia avvenuta o meno una modifica. Siamo però convinti, che per un database sostanzialmente statico quale quello di autenticazione, una strategia del genere porterebbe a un maggiore spreco di risorse. Si pensi infatti, che un operazione di replica comporta la cifratura del database (con la Master Key) sul master, la decifratura sullo slave nonché traffico di rete

Predisporre l'accettazione delle repliche su AFS01 e AFS02

Per accettare le repliche provenienti da SIRIO su AFS01 e AFS02 è necessario attivare il demone hpropd che
ascolta sulla porta 754. Essendo questo servizio "wrappabile" abbiamo deciso di utilizzare il tcpwrapper
inserendo il seguente file (hprop) nella directory /etc/xinet.d:

```
service krb5_prop
{
        flags           = REUSE
        socket_type             = stream
        wait            = no
        user            = root
        server          = /usr/heimdal/libexec/hpropd
        log_on_failure  += USERID
        disable         = no
}
```

ed aggiungendo la linea hpropd:all al file hosts.deny e la linea hpropd:sirio.le.infn.it al file hosts.allow
permettendo così l'accettazione delle repliche soltanto da SIRIO.
Essendo inoltre hpropd un servizio kerberizzato è necessario aggiungere le chiavi di servizio al file /etc/krb5.keytab con i seguenti comandi:

```
[root@afs01]# /usr/heimdal/sbin/kadmin -l ext hprop/afs01.le.infn.it
[root@afs02]# /usr/heimdal/sbin/kadmin -l ext hprop/afs02.le.infn.it
```

Avviare il servizio KDC di Heimdal su AFS01

La distribuzione di Heimdal non comprende gli script per lo start/stop/restart dei servizi per cui è
necessario inserire il comando

/usr/heimdal/libexec/kdc

all'interno di qualche script che sia avviato al momento del boot, in modo da far partire il
servizio di distribuzione dei ticket in maniera automatica.
Il luogo che ci è sembrato più idoneo allo scopo è stato l'elenco dei servizi controllati dal
bosserver di AFS, e precisamente, in sostituzione del Kaserver che va comunque disabilitato per
evitare conflitti con il KDC Heimdal. Si ottiene ciò, dopo aver ottenuto un token amministrativo,
con i comandi:

```
[root@afs01]# bos stop afs01.le.infn.it kaserver
[root@afs01]# bos delete afs01.le.infn.it kaserver
[root@afs01]# bos create afs01.le.infn.it kdc simple
/usr/heimdal/libexec/kdc
```

Verificare a questo punto che tutto funzioni e che il Kaserver sia stato sostituito dal KDC
Heimdal dando il comando:

Configurare Windows 2000 per l'autenticazione nel Regno Kerberos LE.INFN.IT

Sui Windows 2000 Server che sono Domain Controller del dominio w2k.le.infn.it e su tutti i

Windows 2000 Professional appartenenti a tale dominio, dichiarare che SIRIO è il KDC che

autentica il Regno Kerberos LE.INFN.IT. Per ottenere ciò è necessario dare il comando:

C:>ksetup /addkdc LE.INFN.IT sirio.le.infn.it (effettuare il reboot)

Poi su uno dei Domain Controller è necessario creare il trust bidirezionale non transitivo tra il

regno LE.INFN.IT e il regno W2K.LE.INFN.IT. Ciò si ottiene dallo snap-in "Active Directory

Domains and Trusts". Quindi affinché il trust abbia effetto dare i seguenti comandi su SIRIO:

[root@sirio]# kadmin.local –q "addprinc –pw password krbtgt/W2K.LE.INFN.IT@LE.INFN.IT"

[root@sirio]# kadmin.local –q "addprinc –pw password krbtgt/LE.INFN.IT@W2K.LE.INFN.IT"

usando la stessa password che si è digitata nella costruzione del trust su Windows 2000.

Mappare le identità Kerberos del Regno LE.INFN.IT sugli utenti del dominio w2k.le.infn.it

Utilizzare per ognuno degli utenti presenti nel dominio Windows il comando:

```
C:>ksetup /mapuser username@LE.INFN.IT username
```

In realtà, grazie all'uso dell'interfaccia grafica NETUSER è possibile effettuare questa operazione automaticamente. Infatti quando si inserisce o modifica un utente con Netuser, l'utente viene aggiornato anche in Active Directory di Windows oltre che nel NIS di Unix e pertanto automaticamente mappato sul corrispondente principale Kerberos. Se si vogliono sincronizzare automaticaticamente tutti gli utenti del NIS con quelli di Active Direcory è possibile usare lo script adsyncuser di Netuser come segue:

```
[root@pluto]# ypcat passwd | /netuser/scripts/adsyncuser
```

In questo modo si è tranquilli di avere in Active Directory di Windows gli stessi utenti del NIS di Unix e peraltro già mappati sulle corrispondenti identità Kerberos di LE.INFN.IT

NETUSER per la gestione degli Utenti

Netuser è un un’interfaccia grafica per la gestione degli utenti Unix e

Windows scritta in itcl/tk ed utilizzabile sotto il sistema Linux. Essa permette di:

- Creare un’entità Kerberos 5 da associare all’utente
- Creare l’utente AFS
  - Creare un entry nel PTS di AFS
  - Creare la Home Directory dell’utente
  - Assegnare l’utente al gruppo di appartenenza
- Creare un entry nel NIS
- Assegnare l’e-mail all’utente
- Creare l’utente in Active Directory di Windows 2000
- Mappare l’utente Windows 2000 sulla corrispondente identità Kerberos
- Variare la password, la quota disco, l’indirizzo di posta elettronica e il gruppo di appartenenza dell’utente

NETUSER v1.0.0 (October 2001) - with AFS, Kerberos 5, NIS, LDAP and Windows 2000 Active Directory extentions

File Edit Setup Help

ADD EDIT DEL ADD EDIT DEL Group *

INFN Istituto Nazionale di Fisica Nucleare

Passwd

Find

Sync

Print

Log

Exit

Setup

UM	USER	GROUP	DESCRIPTION	UID
1	alessand	studenti	Roberto Alessandi	20366
2	alfinito	gruppo4	Eleonora Alfinito	20228
3	alpha	dipfis	Associazione ALPHA	20400
4	anguiano	gruppo4	Marta Anguiano	7023
5	anni	gruppo4	Raimondo Anni	20229
6	antolini	gruppo2	Roberta Antolini	20332
7	argo	gruppo2	ARGO common Account	20337
8	astro	dipfis	ASTRO common Account	20246
9	beccaria	gruppo4	Matteo Beccaria	20333
10	berna	gruppo2	Paolo Bernardini	20351
11	bianco	perfcour	Maristella Bianco	20371
12	biancom	studenti	Michele Bianco	7198
13	bisconti	studenti	Cristian Bisconti	20410
14	blanco	astro	Armando Blanco	7059
15	bleve	gruppo2	Carla Bleve	20359
16	bogdanov	gruppo4	Leonid.Bogdanov	7024

Log

```
   * /afs/le.infn.it/user/f/fulvio/netuser/scripts/nisUpdate
OK NIS & LDAP successfully updated
   Updating Windows 2000 Active Directory
OK Windows 2000 Active Directory successfully updated
... User fulvio successfully updated
```

Software developed by INFN LECCE - October 2001

NETUSER v1.0.0 (October 2001) - with AFS, Kerberos 5, NIS, LDAP and Windows 2000 Active Directory extentions

File Edit Setup Help

ADD EDIT DEL ADD EDIT DEL Group *

INFN Istituto Nazionale di Fisica Nucleare

Passwd

Find

Sync

Print

Log

Exit

Setup

UM	USER	GROUP	DESCRIPTION
1	alessand	studenti	Roberto Alessandi
2	alfinito	gruppo4	Eleonora Alfinito
3	alpha	dipfis	Associazione ALPHA
4	anguiano	gruppo4	Marta Anguiano
5	anni	gruppo4	Raimondo Anni
6	antolini	gruppo2	Roberta Antolini
7	argo	gruppo2	ARGO common Account
8	astro	dipfis	ASTRO common Account
9	beccaria	gruppo4	Matteo Beccaria
10	berna	gruppo2	Paolo Bernardini
11	bianco	perfcour	Maristella Bianco
12	biancom	studenti	Michele Bianco
13	bisconti	studenti	Cristian Bisconti
14	blanco	astro	Armando Blanco
15	bleve	gruppo2	Carla Bleve
16	bogdanov	gruppo4	Leonid.Bogdanov

*
afsadm
astro
atlas
bussola
dipfis
dipmat
facolta
gruppo1
gruppo2
gruppo3
gruppo4
gruppo5
infnle
kloe
mgr
perfcour
radiaz
roma1
studenti
visitors

Log

```
   * /afs/le.infn.it/user/f/fulvio/netuser/scripts/nisUpdate
OK NIS & LDAP successfully updated
   Updating Windows 2000 Active Directory
OK Windows 2000 Active Directory successfully updated
... User fulvio successfully updated
```

Software developed by INFN LECCE - October 2001

NETUSER v1.0.0 (October 2001) - with AFS, Kerberos 5, NIS, LDAP and Windows 2000 Active Directory extentions

File Edit Setup Help

ADD EDIT DEL ADD EDIT DEL Group *

UM USER GROUP DESCRIPTION UID

INFN Istituto Nazionale di Fisica Nucleare

Passwd

Find

Sync

Print

Log

Exit

Setup

Fulvio Ricciardi

fulvio

User Description

Fulvio Ricciardi

Username

fulvio

Primary Group

afsadm

Enabled

Passwd

Home Directory

/afs/le.infn.it/user/f/fulvio

Shell

sh

csh

tcsh

other

Max Quota (KB)

5000000

Used Quota (51%)

2574309

Ticket life

30

E-mail address

Fulvio.Ricciardi@le.infn.it

Mail Server

mbox.le.infn.it

Mail User

fulvio

Maildrops

OK Apply Cancel Log

... User fulvio successfully updated

Software developed by INFN LECCE - October 2001

NETUSER v1.0.0 (October 2001) - with AFS, Kerberos 5, NIS, LDAP and Windows 2000 Active Directory extentions

File Edit Setup Help

ADD EDIT DEL ADD EDIT DEL Group afsadm

UM USER GROUP DESCRIPTION UID

Enrico M.V. Fasanelli enrico

User Description

Enrico M.V. Fasanell

Username

enrico

Passwd

Home Directory

/afs/le.infn.it/user/e/er

Max Quota (KB)

90000000

Shell

sh

csh

tcsh

other

E-mail address

Enrico.M.V.Fasanelli

Maildrops

OK

Log

Maildrops of user enrico

Enrico.M.V.Fasanelli:maildrop enrico@mbox.le.infn.it
Enrico.MV.Fasanelli:maildrop enrico@mbox.le.infn.it
Enrico.Fasanelli:maildrop enrico@mbox.le.infn.it
enrico:maildrop enrico@mbox.le.infn.it
fasanelli:maildrop enrico@mbox.le.infn.it
root:maildrop enrico@mbox.le.infn.it

OK

Pass

Fir

Syn

Pri

Lo

Ex

Setup

Software developed by INFN LECCE - October 2001

setup

Netuser Root Directory	/afs/le.infn.it/user/f/fulvio/netuse
DNS Domain	le.infn.it

- [x] AFS
- [x] Kerberos 5
- [x] NIS
- [ ] LDAP
- [x] W2K Active Directory

- [x] Sendmail Map
- [x] Mailbox Directory
- [x] Log on Syslog
- [x] SSH Log

W2K DNS Domain	w2k.le.infn.it
AFS Server	afs2.le.infn.it
Kerberos 5 Server	kerberosMIT.le.infn.it
NIS Server	afs2.le.infn.it
NIS Map Directory	/var/yp/NISMASTER
LDAP Server	afs2.le.infn.it
Active Directory Server	w2k-srv3.le.infn.it
Sendmail Server	osfserver.le.infn.it
Sendmail Mailmap File	/etc/mail/userdb
Mailbox Server	mbox.le.infn.it
Mailbox Root Directory	/var/imap

SSH Private Key	/etc/netuser/sshkey/netuser
AFSWS Directory on AFS Server	/usr/afsws
LDAP Administrator	Manager
LDAP Administrator Password	******
Active Directory Administrator	Administrator
Active Directory Admin Password	*******
Default Group	dipfis
Default Ticket Life (days)	30
Default Max Quota (KB)	100000
Default Shell	/bin/tcsh
Default User Password	CambiamiSubito

SAVE CONFIGURATION | RESTORE OLD CONFIGURATION | EXIT

NETUSER LOG VIEW

```
............ User maruccio successfully updated
26 Nov 08:37 Updating user maruccio
............ Nothing to update for user maruccio
26 Nov 08:38 Creating user semeraro
          => Creating Kerberos 5 entry
             * SSH connection to kerberosMIT.le.infn.it for executing the following command:
             * /afs/le.infn.it/user/f/fulvio/netuser/scripts/krb5Create semeraro 30 1
          OK Kerberos 5 entry successfully created
          => Creating AFS entry
             * SSH connection to afs2.le.infn.it for executing the following command:
             * /afs/le.infn.it/user/f/fulvio/netuser/scripts/afsCreate semeraro studenti /afs/le.inf
          OK AFS entry successfully created
          => Creating NIS & LDAP entries
             * SSH connection to afs2.le.infn.it for executing the following command:
             * /afs/le.infn.it/user/f/fulvio/netuser/scripts/nisUpdate
          OK NIS & LDAP entries successfully created
          => Creating Windows 2000 Active Directory entry
          OK Windows 2000 Active Directory entry successfully created
............ User semeraro successfully created
26 Nov 08:40 Creating user salamida
          => Creating Kerberos 5 entry
             * SSH connection to kerberosMIT.le.infn.it for executing the following command:
             * /afs/le.infn.it/user/f/fulvio/netuser/scripts/krb5Create salamida 30 1
          OK Kerberos 5 entry successfully created
          => Creating AFS entry
             * SSH connection to afs2.le.infn.it for executing the following command:
             * /afs/le.infn.it/user/f/fulvio/netuser/scripts/afsCreate salamida studenti /afs/le.inf
          OK AFS entry successfully created
          => Creating NIS & LDAP entries
             * SSH connection to afs2.le.infn.it for executing the following command:
             * /afs/le.infn.it/user/f/fulvio/netuser/scripts/nisUpdate
          OK NIS & LDAP entries successfully created
          => Creating Windows 2000 Active Directory entry
          OK Windows 2000 Active Directory entry successfully created
............ User salamida successfully created
```