Spring HEPiX-HEPNT 2002

W2K Integration in the Kerberos5 based AFS cell le.infn.it

Enrico M. V. Fasanelli

I.N.F.N. – Sezione di Lecce

Catania, 15-4-2002

Outline

- A bit of history
- The integration “idea”
- Summary of results from various tests
- The solution adopted
- Future work

The framework

- Completely separate UNIX & Windows worlds
  - le.infn.it Transarc AFS cell
    - Mainly UNIX clients
      - AIX, HP-UX, DUX, Linux
    - Some WNT4 workstation clients in workgroup
      - CASPUR version of MS-GINA for AFS authentication
      - Login with AFS username mapped to Guest Windows account
  - INFN-NICE WNT4 environment
    - Limited to administrative and CADM users
  - No password synchronization
  - Common services (Web, mail) belongs to unix world
    - Need of a AFS account
    - Some operations (change of password) can be done only in a UNIX machine

The goal

- Single account database for
  - UNIX & Windows
  - Mail (IMAP4, POP)
- Single shared file system
  - Web personal home pages
- Password synchronization
  - Windows users can forget the existence of unix

Constraints for the new solution

- From the UNIX point of view
  - Must save existing AFS infrastructure
  - Must be available on all platform in use
  - Better if free/OpenSource
- From Windows side
  - Must works with Windows 2000
  - Don’t care about W9x & WNT4
- Don’t write ad hoc code

Kerberos !

- Seems to be the only common infrastructure
  - Windows authentication in

W2K Kerberos

- PROS
  - Native authentication for the Windows world
  - Can authenticate a properly configured Unix Kerberos5 client
- CONS
  - No way to get AFS tokens

MIT Kerberos 5

- PROS
  - Is known to works with Windows 2000
    - There is a Microsoft step-by-step guide to do this [1]
  - Can provide AFS tokens (via external “`fakeka`” [2] utility)
- CONS
  - Windows AFS clients think to be in the year 1601 if the tokens lifetime is greater than 12 hours
  - Old Unix AFS clients (afs3.4 build 5.28) do not authenticate

KTH Heimdal

- PROS
  - Native and well behaved AFS support
  - Authenticate Windows login
- CONS
  - Authenticated users cannot access the shared resources in the W2K domain
  - Windows AFS clients work in a strange way
    - Get the tokens, but Windows say that AFS service cold not be started!!!

Null intersection

- Windows 2000 AD need Windows Kerberos5
- Windows 2000 works ONLY with MIT Kerberos5 based realm
- The AFS client in a W2K machine works ONLY with HEIMDAL Kerberos5
- Unix AFS clients works with both MIT and HEIMDAL
  - The inter-cell communication is done in native way in HEIMDAL and instead needs the “external” `fakeka` in MIT

Union: Windows + MIT + HEIMDAL

- AD Windows 2000 domain w2k.le.infn.it
  - We need a domain name (realm) different from the one hosting AFS cell in order to make the trust relationship
- Kerberos5 realm LE.INFN.IT served by an MIT KDC
  - AFS cell is le.infn.it
- Define a trust relationship between them
  - On Windows side (W2K.LE.INFN.IT KRB5 realm)
    - Ksetup
    - Active Directory Domains and Trusts
  - On LE.INFN.IT KDC
    - Kadmin for adding principals krbtgt/W2K.LE.INFN.IT@LE.INFN.IT and krbtgt/LE.INFN.IT@W2K.LE.INFN.IT

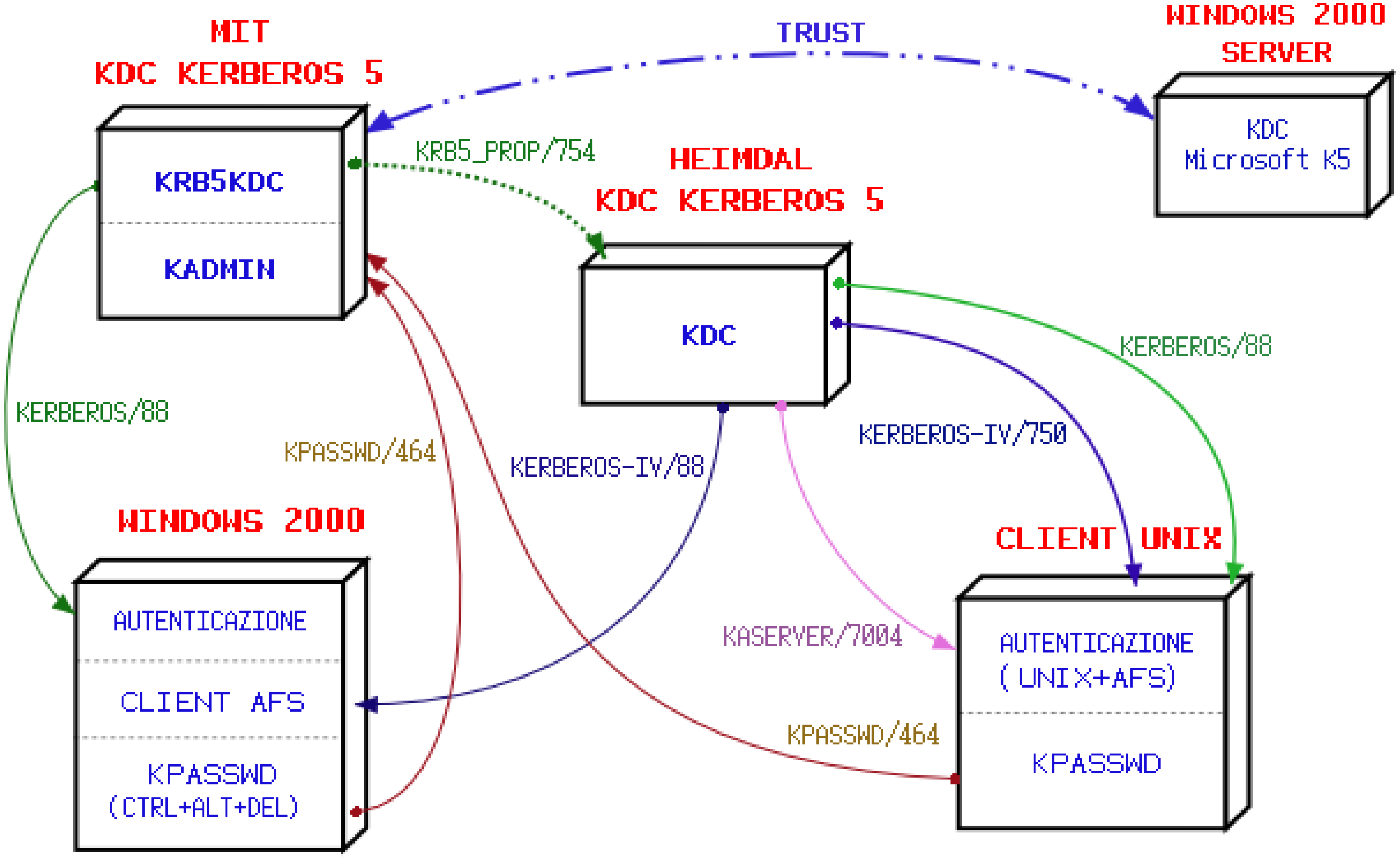
From AFS KAserver to MIT KDC I

- Configured the LE.INFN.IT Kerberos5 realm based to the MIT master KDC
  - We use MIT Kerberos 5 version 1.2.2 on a Linux RH 7.2
- Populated the KDC principal database with AFS database entries using afs2k5db, a tool from Ken Hornstein's migration kit [2]
- Configured the AFS db servers in order to run HEIMDAL in slave mode
  - This is done inside BOS configuration

From AFS KAserver to MIT KDC II

- Configured the master LE.INFN.IT KDC in order to propagate any database change to the slaves ones (HEIMDAL based)
- Modify database related commands (klog, kpasswd, ecc.) in all unix AFS clients with the corresponding kerberized ones

A simple picture



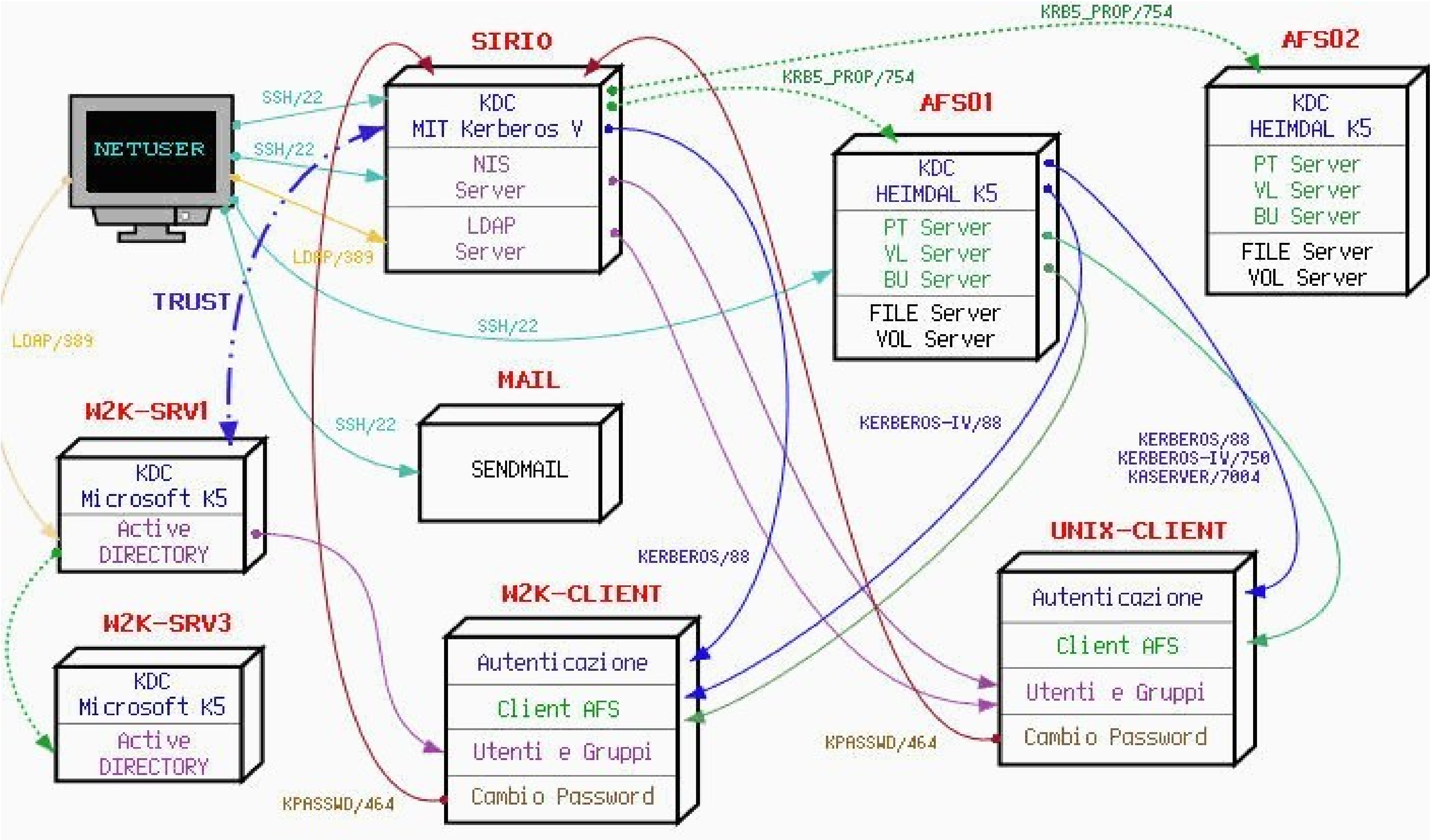
Windows configuration

- Windows 2000/XP professional belongs to w2k.le.infn.it AD domain
- Ksetup at installation time advertise the LE.INFN.IT kerberos realm
- Users login in the LE.INFN.IT realm with their AFS username/password
  - The windows authentication is done via the trust relationship of two realms
  - The AFS client get the token at login time
- Startup script maps AFS home to assigned network drive

Windows user administration

- Mapping between AFS user and the Windows one allow AD resources usage
- By default users have a pre-assigned (unknown to the user) password in the AD domain and then their can login only in the LE.INFN.IT realm
- Ctrl+Alt+Del sequence permit to change the Kerberos password

A more complicated view



w2k.le.infn.it domain

- Windows AD domain is used to
  - Share resources (printers)
  - Deploying anti virus
- Is not used for login
  - Users login in the LE.INFN.IT Kerberos realm
  - Users don’t know their AD domain password
- Problems with laptop disconnected from the network
  - Workaround: enable domain login

Opened issues

- Laptops
  - Disconnected login
  - OpenAFS client on Windows XP

References/Useful links

[1] Microsoft step-by-step guide to kerberos 5

http://www.microsoft.com/windows2000/techinfo/planning/security/kerbsteps.asp

[2] Ken Hornstein migration kit

ftp://ftp.cmf.nrl.navy.mil/pub/kerberos5/afs-krb5-1.3.tar.gz

[3] KTH HEIMDAL

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

[4] KTH Kerberos 4

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

[5] MIT Kerberos 5