HIMSS and RSNA
Integrating the Healthcare Enterprise

Kerberos Notes

Electronic Radiology Laboratory
Mallinckrodt Institute of Radiology
510 South Kingshighway Blvd.
St. Louis, MO 63110
314.362.6965 (Voice)
314.362.6971 (Fax)

Revision 7.3.0
November 11, 2003

1 Introduction 3
2 Configuration of Windows 2000 Server as Kerberos Authentication Server 3
3 Configuration of RedHat 9 Linux Workstation as Kerberos Authentication Client 4

1 Introduction

This document provides notes about Kerberos software, servers, installation, and any other information we can think to provide. Some of the notes include references to systems installed at Washington University. That is done both as a reminder to us and to provide concrete examples.

2 Configuration of Windows 2000 Server as Kerberos Authentication Server

1. Install Active Directory (which also installs DNS).
2. Configure a domain name as this sytem will act as a domain controller. *(The domain name chosen for the WU private network is WUSTL.EDU.)*
3. Configure DNS for forward and rever lookup zones. For convenience, a pointer record is added to the reverse lookup zone for this system (which is now a DNS server). *(At WU, we also added an entry for the Linux host used in our experiments.)*
4. Use the Active Directory service management tool to create an Organizational Unit called "Accounts". The "Accounts" Organizational Unit is under "Active Directory Users and Computers | wustl.edu".
5. In the "Accounts" Organizational Unit, add a user. The test plans call for the name *khimss*.
6. The Kerberos configuration utilities are in C:\Program Files\Support Tools. Run the ktpass program to create a keytab file on the Windows 2000 server. (This keytab file will be copied over to the Linux host, and merged with */etc/krb5.keytab*). The ktpass command was used to create a keytab file and set the password. In the example below, the host name is ihe-2.

```
C:\Program Files\Support Tools>ktpass -princ host/ihe-
2.wustl.edu@WUSTL.EDU -mapuser ihe-2 -pass 1234AaBb -out
C:\ihe-2.keytab
Successfully mapped host/ihe-2.wustl.edu to ihe-2.
Key created.
Output keytab to C:\ihe-2.keytab:
Keytab version: 0x502
keysize 57 host/ihe-2.wustl.edu@WUSTL.EDU ptype 1
(KRB5_NT_PRINCIPAL) vno 1 etyp e 0x1 (DES-CBC-CRC)
keylength 8 (0xb50b084c2f764080)
Account has been set for DES-only encryption.
```

The steps above allowed us to create an ihe-2 account and a keytab file with that information. At a later time, we created the khimss account and did not regenerate the keytab file. The Linux system was able to authenticate the khimss acount without installation of a new keytab file.

3 Configuration of RedHat 9 Linux Workstation as Kerberos Authentication Client

1. Install from the RedHat CDs and use the "custom" configuration option. (You can always configure after the fact if you miss this step.) During the installation, the authentication configuration should include shadow passwords, md5 passwords; and must include Kerberos 5 to authenticate using the Windows 2000 server. For Kerberos to work, we also need to specify the Realm, KDC, and Admin Server.
2. The Realm is whatever the Active Directory domain was configured to be, except in uppercase. In the example below, the hostnames are registered with a DNS server that is not the KDC/Kerberos Authentication Server.

   ```
   Realm:          WUSTL.EDU
   KDC:       ihe-3.wustl.edu:88
   Admin Server:  ihe-3.wustl.edu:749
   ```

3. Copy the keytab file created on the Kerberos Authentication Server and install on this system. These steps were performed as root using the keytab file *ihe-2.keytab*:

   ```
   unix-prompt> # ktutil
   ktutil:  rkt ihe-2.keytab
   ktutil:  list
   slot KVNO Principal
   ---- ---- ---------------------------------------------------------------------
      1    1          host/ihe-2.wustl.edu@WUSTL.EDU
   ktutil:  wkt /etc/krb5.keytab
   ktutil:  q
   ```

4. Add a user on the local unix box. This should be the same user that was added on the Kerberos Authentication Server. Lock the password entry on the local unix system. This should force the system to use the Kerberos Authentication Server.
5. Logon to the Unix system using the account created (khimss).
6. Run the command klist to list Kerberos tickets.

7. Logoff and disconnect the network adapter. Try to login again using the account created. This step should fail because you no longer have a connection to the Kerberos Authentication Server.