LAB:
Implementing Single Sign-on
!!!Setup!!!

ITSO iSeries Technical Forum - 2003

This publication may refer to products that are not currently available in your country.
IBM makes no commitment to make available any products referred to herein.

Purpose and Overview of EIM

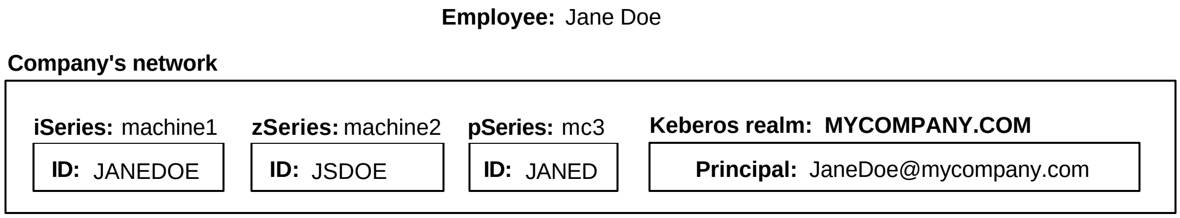
Purpose of EIM

When a system or server uses network authentication (i.e. Kerberos tickets) rather than a local ID and password for user authentication, the system or server must determine what local ID to use after a successful authentication. EIM was created to simply the process of determining who to become after a successful network authentication.

Overview of EIM

In V5R2, IBM introduced Enterprise Identity Mapping (EIM). This is a function that crosses IBM eServer platforms. EIM is a building block function. EIM doesn't do any authentication or authorization checking. EIM is a set of APIs and GUI interfaces that allow an administrator to create and maintain a list of people within an enterprise and keep track of what IDs are associated with the person on various systems in the network. EIM maps user identities between systems. Applications can use the mappings to decide what local ID to use after a network authentication. Below is an example of how the EIM directory could be set up for a user.

A company maintains a computer network with 3 machines, all of which participate in a Kerberos realm. Within the network, an employee has an ID on each system, as well as a Kerberos principal name.



Employee: Jane Doe

Company's network

iSeries: machine1 — **ID:** JANEDOE

zSeries: machine2 — **ID:** JSDOE

pSeries: mc3 — **ID:** JANED

Keberos realm: MYCOMPANY.COM — **Principal:** JaneDoe@mycompany.com

In this example, you may want to create the following EIM associations for the employee Jane Doe.

List Of EIM Associations for Jane Susan Doe			
EIM Identifier	**Registry Name**	**Registry User Name**	**Association Type**
Jane S. Doe	MYCOMPANY.COM	JaneDoe@mycompany.com	Source
Jane S. Doe	machine1	JANEDOE	Target
Jane S. Doe	machine2	JSDOE	Target
Jane S. Doe	mc3	JANED	Target

The following terms are used by EIM:

- **EIM Association:** An association is an entry that shows what ID is assigned to a particular person or server in a registry. There is also an association type that indicates how the association is to be used.
- **EIM Identifier:** This is a unique value used to identify a particular person or server. An identifier can have any number of associations.

- **Registry Name:** A registry name refers to a place where a list of valid users or servers is kept. For example, a *registry name* may refer to a computer system, a Kerberos realm, or an LDAP directory.
- **Registry User Name:** This is the local user name assigned to a particular person or server for the registry (place) referenced in the association. For example, a *registry user name* may refer to a user profile, or Kerberos principal name, or an LDAP user.
- **Association Type:** This indicates how the association can be used.
    - **Source:** Having the value of *source* implies that authentication will be done with the registry user name. It also implies the source registry user name will be used to find the target identity for other registries (systems).
    - **Target:** Having the value of *target* implies that authentication was done with a different source registry user name and that a mapping from the source to the target registry user name exists. Generally, these mappings are used to decide what local user "to become".
    - **Source and Target:** This value allows the association to be used for finding other associations and for deciding what local user "to become".

Once the administrator has created and populated the EIM directory, applications can use EIM APIs to retrieve information about Enterprise users. Applications can use the mapping information to determine with which profile to run a function, or to develop tools to help manage users in a large network.

How EIM Associations Are Used After Kerberos Authentications in iSeries Functions

Some iSeries functions have to be enabled to accept Kerberos service-tickets for authentication. However, after an authentication, what local user should be used while running the job? The Kerberos-enabled functions extract the client principal name from the service-ticket. The client principal name becomes the EIM source registry user name. The Keberos-enabled function uses the source registry user name to find the target registry user name on the local system.

Building on the example from the EIM overview section, assume iSeries Navigator is configured to use Kerberos authentication. Jane Doe starts iSeries navigator from her PC. A Kerberos service-ticket is obtained and passed to iSeries Navigator. The authentication code determines that a valid service-ticket has been received from *JaneDoe@MYCOMPANY.COM*. The iSeries Navigator code calls the appropriate EIM APIs to retrieve the target association for the iSeries based off of the source association for *JaneDoe@MYCOMPANY.COM*. The registry user name from the target association contains the OS/400 user profile name that will be used for the jobs iSeries Navigator starts for Jane. EIM did not do the authentication and it did not change the attributes of any jobs. EIM was used to determine what profile to use after authentication. This is the same method used for all the iSeries functions that support Kerberos authentication.

For more information on EIM, refer visit the web site:

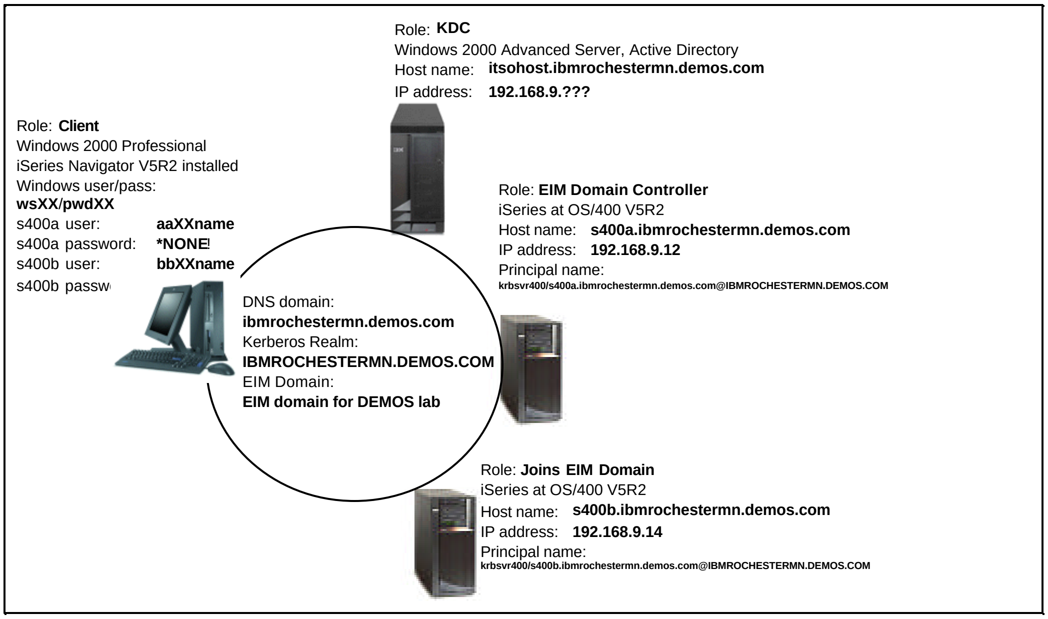
http://publib.boulder.ibm.com/iseries/v5r2/ic2924/index.htm

then follow the links *Networking->Networking Security->Enterprise Identity Mapping (EIM)*.

Abstract

In this lab the student will learn how to configure and exploit a single-sign-on environment. Student lab exercises will include:

1. Configuring iSeries to participate in an EIM domain.
2. Configuring the iSeries to Participate in a Kerberos Realm
3. Configuring EIM associations
4. Connecting to iSeries through iSeries Navigator using Kerberos Authentication. See how EIM associations are used to determine with which profile to run.
5. Access systems through QFileSvr.400 and TELNET. See how EIM associations are used to determine with which profile to run.
6. Working with a Kerberos and EIM enabled application.



Role: **KDC**
Windows 2000 Advanced Server, Active Directory
Host name: **itsohost.ibmrochestermn.demos.com**
IP address: **192.168.9.???**

Role: **Client**
Windows 2000 Professional
iSeries Navigator V5R2 installed
Windows user/pass:
wsXX/pwdXX
s400a user: **aaXXname**
s400a password: ***NONE!**
s400b user: **bbXXname**
s400b passw

DNS domain:
ibmrochestermn.demos.com
Kerberos Realm:
IBMROCHESTERMN.DEMOS.COM
EIM Domain:
EIM domain for DEMOS lab

Role: **EIM Domain Controller**
iSeries at OS/400 V5R2
Host name: **s400a.ibmrochestermn.demos.com**
IP address: **192.168.9.12**
Principal name:
krbsvr400/s400a.ibmrochestermn.demos.com@IBMROCHESTERMN.DEMOS.COM

Role: **Joins EIM Domain**
iSeries at OS/400 V5R2
Host name: **s400b.ibmrochestermn.demos.com**
IP address: **192.168.9.14**
Principal name:
krbsvr400/s400b.ibmrochestermn.demos.com@IBMROCHESTERMN.DEMOS.COM

This lab setup guide will assist the instructor in setting up this environment consisting of two iSeries servers, one kerberos KDC and the client systems.

Prerequisites

iSeries server prerequisites:

- Two physical iSeries
  - One to be the EIM domain and the other to join the EIM domain. This could be one physical system using LPAR, of course.
  - Each connected to a LAN (ethernet or TRN - does not matter)
- 5722-SS1 - V5R2 of OS/400

    - Include the latest and greatest CUM PTF package
- 5722-AC3 - Crypto Access Provider
- 5722-XE1 - iSeries Access for Windows
- Library SETUPEIMDE is used to create the lab environment (userids, etc)

Kerberos server prerequisites:

- Windows 2000 Server
    - Service Pack 3
        - Plus, you might want to try to find other security patches as a Windows server is riddled with security bugs and flaws.
    - Active Directory
    - Windows Support Tools (must have for the ktpass command)
    - Optional: DNS server is an optional tool to allow you to travel to a new lab environment and not be dependant on the local name to IP address mappings. It is not necessary, however. An iSeries DNS can be used too, but a little bit harder to carry on the airplane!

Windows client prerequisites:

- Windows 2000
- iSeries Navigator
    - Must include Network and Security options (best is simply to include all)
    - Must use 5250 Emulator built into iSeries Navigator (not Personal Communications) for the display emulator session to the iSeries. This is because Personal Communications does not yet support Kerberos authentication.

General Lab Information

The following preparatory steps have been completed for you:

- All the necessary SW prerequisites are installed.
- Your PC has been configured to participate in the Kerberos realm GARRY.COM
- The iSeries **s400a** and **s400b** have been configured to participate in the EIM domain for COMMON.
- Lab user profiles are created.
- Lab user profiles are authorized to the necessary directories.
- Example data is primed in the directories.
- Static mappings for were added for **s400a** and **s400b** using the *properties* button from iSeries Navigator link *Security->Network Authentication Service*. The mappings were added from the *host resolution* property sheet. This is done to map the iSeries DNS name to the Kerberos realm.

The iSeries systems you will use in this lab are: **s400a** and **s400b**.

The PC you are using has a unique 2-digit number assigned to it which is displayed on a sheet of paper. You will use this number in your user profile and password to maintain uniqueness between students during the lab. You will replace XX with your 2-digit number.

In addition to your workstation ID, you will be using OS/400 profiles on **s400a** and **s400b**, and a series of principals from a Kerberos realm.

The naming convention for the OS/400 profiles are listed below. You will replace XX with your 2-digit work station number. The OS/400 user profiles have the special authorities *ALLOBJ, *SECADM, and *IOSYSCFG which are needed to run the configuration wizards.

Your OS/400 *USRPRF	eimXX	**eim_____**
Your OS/400 *USRPRF Password	eimXXpw	**eim____pw**

The naming convention for the Kerberos principals for the domain GARRY.COM are listed below. In this lab you will map wsXX to profiles on the **s400a** and **s400b** systems.

Your GARRY.COM Kerberos Principal	wsXX	**eim_____**
Your principal's password	eimXX	**eim_____**

Common Variables

<Kerberos.name>:	itsohost
<Kerberos.IPaddr>:	n.n.n.n

<DNS.server.IPaddr>:	x.x.x.x Note: this is the IP address of your KDC server too, most likely
<DNS.domain>:	ibmrochestermn.demos.com
<DNS.forwarder>:	9.10.244.100

<s400a.oldname>:	opsb
<s400a.olddomain>:	rchland.ibm.com
<s400a.newname>:	s400a
<s400a.PTR>:	9.5.173.198 as opsb.rchland.ibm.com. Note: What is the CFGTCP option 12 host name?
<s400a.IPaddr>:	9.5.173.198

<s400b.oldname>:	opsd
<s400b.olddomain>:	rchland.ibm.com
<s400b.newname>:	s400b
<s400b.PTR>:	9.5.173.200 as opsd.rchland.ibm.com Note: What is the CFGTCP option 12 host name?
<s400b.IPaddr>:	9.5.173.200

iSeries Setup

Follow these steps on both iSeries (s400a and s400b)

□ CHGSYSVAL QRMTSIGN *SAMEPRF (or *VERIFY)

Restore SETUPEIMDE library

All the setup stuff you need is in the file: setupeimde/qclsrc.

I am including the savf of the setupeimde/qclsrc file. I tested this procedure.

- □ Detach the file.
- □ CRTSAVF SETUPEIMDE (on your target system)
- □ FTP to target system the savf. Of course BINARY option.
- □ CRTLIB SETUPEIMDE (on your target system)
- □ Issue restore: RSTOBJ OBJ(QCLSRC) SAVLIB(SETUPEIMDE) DEV(*SAVF) OBJTYPE(*FILE) SAVF(SETUPEIMDE) FILEMBR((*ALL *ALL)) MBROPT(*ALL) ALWOBJDIF(*ALL)
- □ Issue crt: CRTBNDCL SETUPEIMDE/DEMOPRF SETUPEIMDE/QCLSRC
- □ Build profiles and base objects needed: call setupeimde/demoprf ('crt' 'a' 'x')

It assumes the source files it needs are also in SETUPEIMDE/QCLSRC. If you want to rename the library, you will have to change the DEMOPRF program also. The program takes three parms: The action (CRT or DLT), The system ID (a or b), and parm that only has meaning when the action is DLT. The third parameter indicates you want to delete the everything, or just the objects the test profiles own. It will be clearer in a minute:

```
call setupeimde/demoprf  ('crt' 'a' 'x')     --- X means nothing.
call setupeimde/demoprf ('dlt' 'a' 'o')      --- o means only delete objects.
call setupeimde/demoprf ('dlt' 'a' 'Y')      --- NOT o means delete profiles and objects.
```

CFGTCP on s400a

Note: It is important to have the 'local name' (for example, opsd and opsd.rchland.ibm.com) either in the host table in lower case or on the DNS server. When you do the kinit -k yadda... to test in QSH one of the reasons you will get an error is if the iSeries cannot resolve to the lower case of the local name.

Note: As shown it should work a bit better if the **Host name search priority** is set to ***REMOTE**. This, then, reduces the errors introduced by the OS/400 host table entries where, in lab environment, everybody is changing.

CFGTCP option 12:

```
- - - - - -             Change TCP/IP Domain (CHGTCPDMN)

 Type choices, press Enter.

 Host name  . . . . . . . . . . .   'opsb' <s400a.oldname>

 Domain name  . . . . . . . . . .   'rchland.ibm.com' <s400a.olddomain>



 Domain search list . . . . . . .   'ibmrochestermn.demos.com rchland.ibm.com'
  <DNS.domain> <s400a.olddomain>


 Host name search priority  . . .   *REMOTE        *REMOTE, *LOCAL, *SAME
 Domain name server:
   Internet address . . . . . . .   '9.10.109.80'  <DNS.server.IPaddr>
                                    '9.10.244.100'  <DNS.forwarder>
                                    '192.168.9.5'
```

CFGTCP option 10:

```
- - - - - -       Work with TCP/IP Host Table Entries
                                                            System:   OPSB
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   7=Rename
```

```
     Internet          Host
Opt  Address           Name

     9.5.173.198       OPSB.RCHLAND.IBM.COM
                       OPSB
     127.0.0.1         LOOPBACK
                       LOCALHOST
```

CFGTCP on s400b

Note: It is important to have the 'local name' (for example, opsd and opsd.rchland.ibm.com) either in the host table in lower case or on the DNS server. When you do the kinit -k yadda... to test in QSH one of the reasons you will get an error is if the iSeries cannot resolve to the lower case of the local name.

Note: As shown it should work a bit better if the **Host name search priority** is set to ***REMOTE**. This, then, reduces the errors introduced by the OS/400 host table entries where, in lab environment, everybody is changing.

CFGTCP option 12:

```
- - - - - -              Change TCP/IP Domain (CHGTCPDMN)

 Type choices, press Enter.

 Host name  . . . . . . . . . . .   'opsd' <s400b.oldname>

 Domain name  . . . . . . . . . .   'rchland.ibm.com' <s400b.olddomain>



 Domain search list . . . . . . .   'ibmrochestermn.demos.com rchland.ibm.com'
  <DNS.domain> <s400b.olddomain>


 Host name search priority  . . .   *REMOTE        *REMOTE, *LOCAL, *SAME
 Domain name server:
   Internet address . . . . . . .   '9.10.109.80'  <DNS.server.IPaddr>
                                    '9.10.244.100'  <DNS.forwarder>
                                    '192.168.9.5'
```

CFGTCP option 10:

```
- - - - - -           Work with TCP/IP Host Table Entries
                                                            System:   OPSD
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   7=Rename

     Internet          Host
Opt  Address           Name

     9.5.173.200       OPSD
                       OPSD.RCHLAND.IBM.COM
     127.0.0.1         LOOPBACK
                       LOCALHOST
```

Edit krb5.conf file

If you have a problem with the QFileSvr.400 lab not working due to authentication problem - you will need to edit the krb5.conf file (on both iSeries)

□ wrklnk('/qibm/userdata/os400/networkauthentication/krb5.conf')

□ 2=Edit

□ Add a second domain_realm so you have one for both iSeries servers. That is, you should have two that look somthing like this:

```
??(domain_realm??)
  opsb.rchland.ibm.com= IBMROCHESTERMN.DEMOS.COM
  opsd.rchland.ibm.com= IBMROCHESTERMN.DEMOS.COM
```

Windows 2000 Server Setup

Follow these steps to configure the Windows 2000 DNS and Kerberos KDC servers.

Configure the DNS server (setup)

Use these values. Any changes you make you must make everywhere! And, of course, the DNS server could (should?) very well be on one of the iSeries!

Use the information found here:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/csvr2002/htm/cs_dp_installexamples_nluw.asp
to configure the Active Directory and DNS on your Windows 2000 Server. Select step 1.

Our modifications to the Microsoft words are done in <***bold italics***>.

- - - - -

Commerce Server 2002

Step 1: Configure Active Directory and DNS on Computer 1

You configure the first computer for Active Directory and DNS, and then promote it to an Active Directory domain controller. Active Directory will store sensitive user profile data such as user name and password. The remaining non-sensitive profile data will be stored in the SQL Server database.

To configure Computer 1

□ Install Windows 2000 Advanced Server, using the **Default** installation.

- Use only alphanumeric characters in the computer name.
- Format the partition with Windows NTFS file system where Windows 2000 is to be installed.
- Make sure that **Internet Information Services (IIS)** is **not** selected in the **Windows 2000 Components** screen.

□ Install Windows 2000 Service Pack ***<3 (SP3)>*** and the required hotfixes specified at http://go.microsoft.com/fwlink/?LinkId=6125.

□ Open **Control Panel**, and then use **Network and Dial-up Connections** to configure the static **Internet Protocol (IP) address**, **Subnet mask**, and **Default gateway**. Use the static IP address of the domain controller as the **Preferred DNS Server**. For detailed instructions, see "Configure TCP/IP to use DNS" and "Configure TCP/IP to use WINS" in Windows 2000 Server Help.

For additional networking information, see the *Microsoft Windows 2000 Server Resource Kit*.

To promote Computer 1 to an Active Directory domain controller, you must use the Active Directory Installation Wizard to specify that this computer is the domain controller.

To promote Computer 1 to a domain controller

□ Click **Start**, and then click **Run**.

□ In the **Run** dialog box, in the **Open** box, type **dcpromo**, and then click **OK**.

□ In the **Active Directory Installation Wizard**, click **Next**.

□ In the **Domain Controller Type** dialog box, select **Domain controller for a new domain**, and then click **Next**.

□ In the **Create Tree or Child Domain** dialog box, select the **Create a new domain tree** option, and then click **Next**.

□ In the **Create or Join Forest** dialog box, select **Create a new forest of domain trees**, and then click **Next**.

□ In the **New Domain Name** dialog box, in the **Full DNS name for new domain** box, type the full DNS name for the new domain (for example, wideworldimporters.com). ***<We used IBMROCHESTERMN.DEMOS.COM>***

□ In the **NetBIOS Domain Name** dialog box, in the **Domain NetBIOS name** box, type the name (for example, wideworldimporters) that users of earlier versions of Windows will use to identify the domain. It is recommended that you accept the default, which is a shortened version of the full DNS name. Click **Next**.

□ In the **Database and Log Locations** dialog box, select the location where you want to place your log files.

□ In the **Shared System Volume** dialog box, accept the default settings, unless you have a specific reason to change them.

□ If DNS is not installed on your computer, you will be prompted to install it. Select **Yes, install and configure DNS on this computer**, and then click **Next**.

□ In the **Permissions** dialog box, select the **Permissions compatible only with Windows 2000 servers** option, and then click **Next**.

□ In the **Directory Services Restore Mode Administrator Password** dialog box, do the following:

Use this	**To do this**
Password	Type the password that you want to assign to the Administrator account for the server.

Confirm password Type the password again to confirm it.

- □ Click **Next**.
- □ In the **Summary** dialog box, review the options you selected to ensure your Active Directory configuration is correct. If it is, click **Next** to start the installation process, or to reconfigure your selections, click **Back**.
- □ During the installation process, you might be required to insert the Windows 2000 CD into the CD-ROM drive.
- □ In the **Completing the Active Directory Installation Wizard** dialog box, click **Finish**.
- □ Restart the server.

Configure the DNS server (continued)

Continue to configure the DNS server for your environment:

- □ Right click **Forward Lookup Zones** and select **New Zone** from the context menu. Create a new primary zone named **ibmrochestermn.demos.com.** (trailing period is significant).
- □ Right click the Forward Lookup Zone **ibmrochestermn.demos.com.** and select **Other New Records...** from the context menu. On the **Resource Record Type** panel select **Service Location** to create an SRV record. Click **Create Record**. Complete the panel:
  - □ Service: **_kerberos**
  - □ Protocol: **_udp**
  - □ Priority: **0**
  - □ Weight: **0**
  - □ Port number: **88**
  - □ Host offering this service: **itsohost.** (trailing period is significant)
- □ If you are operating in a bigger 'DNS scheme' you will want your traveling DNS server to forward requests that it cannot handle to the 'site' DNS. To do this right click **itsohost** and select **Properties** from the context menu. On the **Forwarders** tab, select **Enable forwarders** and then add any (and all) IP addresses. For example, **<DNS.forwarder>**.
- □ Right click **<DNS.domain>** and select **New Host...** from the context menu. Add a Host (or A record) for:
  - □ Name: s400a <s400a.newname>
  - □ IP address: 9.5.173.198 <s400a.IPaddr>
- □ Right click **<DNS.domain>** and select **New Host...** from the context menu. Add a Host (or A record) for:
  - □ Name: s400b <s400b.newname>
  - □ IP address: 9.5.173.200 <s400b.IPaddr>
- □ Right click **<DNS.domain>** and select **New Host...** from the context menu. Add a Host (or A record) for:
  - □ Name: itsohost <Kerberos.name>
  - □ IP address: n.n.n.n <Kerberos.IPaddr>
- □ Right click **Reverse Lookup Zones** and select **New Zone** from the context menu. Create a new primary zone for n.n.n.x (where this is a logical subnet of your network.
- □ Right click **n.n.n.x Subnet** and select **New Pointer** from the context menu. Create a reverse pointer record (PTR) for the **<s400a.IPaddr>** and **<s400a.oldname>.<s400a.olddomain>**. We do this to provide a way for the EIM wizard to map the iSeries host name and domain (which it grabs from the CFGTCP option 12) to the IP address. In a 'normal' situation this would not be necessary.
- □ Right click **n.n.n.x Subnet** and select **New Pointer** from the context menu. Create a reverse pointer record (PTR) for the **<s400b.IPaddr>** and **<s400b.oldname>.<s400b.olddomain>**. We do this to provide a way for the EIM wizard to map the iSeries host name and domain (which it grabs from the CFGTCP option 12) to the IP address. In a 'normal' situation this would not be necessary.

Configure the Active Directory server

Use these values. Any changes you make you must make everywhere!

- □ Expand the **IBMROCHESTERMN.DEMOS.com** domain.

Create new s400a user for krbsvr400

- □ Right click **Users** and select **New** -> **User** from the context menu.
  - □ First name: **krbsvr400s400a**
  - □ Display name: **krbsvr400s400a**
  - □ password: **kerberos**

  Account tab:
  - □ User logon name: **krbsvr400/opsb.rchland.ibm.com @IBMROCHESTERMN0.DEMOS.COM**
  - □ User logon name (pre-Windows 2000): **IBMROCHESTERMN0\ krbsvr400s400a**
  - □ Account options: select **Password never expires**
  - □ Account options: select **Account is trusted for delegation**
- □ From the command line issue (if you make a mistake and need to redo add **-mapOp** set to the end.
  - □ **ktpass -princ krbsvr400/opsb.rchland.ibm.com@IBMROCHESTERMN.DEMOS.COM -mapuser krbsvr400s400a -pass kerberos**

- □ **Create new s400b user for krbsvr400**
  - □ Right click **Users** and select **New** -> **User** from the context menu.
  - □ First name: **krbsvr400s400b**
  - □ Display name: **krbsvr400s400b**
  - □ password: **kerberos**

  Account tab:
  - □ User logon name: **krbsvr400/ops d.rchland.ibm.com @IBMROCHESTERMN0.DEMOS.COM**
  - □ User logon name (pre-Windows 2000): **IBMROCHESTERMN0\ krbsvr400s400b**
  - □ Account options: select **Password never expires**
  - □ Account options: select **Account is trusted for delegation**
- □ From the command line issue (if you make a mistake and need to redo add **-mapOp** **set** to the end.
  - □ **ktpass -princ krbsvr400/ops d.rchland.ibm.com@IBMROCHESTERMN.DEMOS.COM -mapuser krbsvr400s400b -pass kerberos**

Create new team users for wsXX

Note: after you create the first user wsXX you can right click on the Name and select **Copy...** from the context menu. Make sure that the properties of each copied users is correct as not all of the options copy. Specifically it seems that you must select **Account is trusted for delegation**.

- □ Right click **Users** and select **New** -> **User** from the context menu.
  - □ First name: **work**
  - □ Last name: **station XX**
  - □ Display name: **work station 01**
  - □ password: **pwdXX**

  Account tab:
  - □ User logon name: **wsXX @IBMROCHESTERMN0.DEMOS.COM**
  - □ User logon name (pre-Windows 2000): **IBMROCHESTERMN0\ wsXX**
  - □ Account options: select **Password never expires**
  - □ Account options: select **Account is trusted for delegation**

  Member Of tab:
  - □ Make this user a member of **Administrators** in addition to the Domain Users.

□ Make sure all the time skews are correct

These steps are not required for the Network authentication to work. However, by performing these steps, you confirm that the Kerberos environment is working correctly.

Note: The user performing these steps must have a home directory in the IFS. The home directory stores the krb5ccname file, containing the link to the credential cache. While in QSH create a home directory for your user profile with the command: **mkdir /home/<userprofile>**

□ **keytab list**
This lists the current keys in the Kerberos key table. If the wizard completed correctly and made contact with the KDC, it should now contain three entries for the krbsvr400 principal (at different encryption levels). If the principal name of the krbsvr400 service displays a wrong host name, verify that the host table on the PC you are performing the configuration on has the correct entries.

□ **kinit -k krbsvr400/<s400a.oldname><s400a.olddomain>@IBMROCHESTERMN.DEMOS.COM**
This requests a TGT from the KDC. This should complete with out error and return the prompt.

Some errors that could occur at the kinit stage:

- **Unable to obtain name of default credentials cache**: While in QSH create a home directory for your user profile with the command: **mkdir /home/<userprofile>**
- **Unable to obtain initial credentials**
- Status 0x96c73a06 - **Client principal is not found in security registry**: The krbsvr400 principal had been misspelled.
- Status 0x96c73a25 - **Time differential exceeds maximum clock skew**: The KDC was using daylight savings time or the clocks are more than 5 minutes apart.
- Status 0x96c73a9a - **Unable to locate security server**: Realm name resolving incorrectly. Check case sensitivity.

□ **klist**

This lists the tickets in the ticket cache and should display the newly received ticket from the KDC.

Windows 2000 Client Setup

Follow these instructions on the students Windows 2000 client systems.

□ Copy the files cwbunsy.jar, cwbunsyn.jar and sy.jar into c:\Program Files\IBM\Client Access\Classes. These files stub the EIM and Kerberos NAS wizards so the students can see but not change the configuration. Note: This will replace the 'real' programs on the client. If you need to use these system later - you should make a back up of the real files.

□ Make sure the student PCs have the following network configuration:

  □ IP Address of DNS: 192.168.9.84, followed by the 'site' DNS: 192.168.9.5

  □ Domain Search Order: ibmrochestermn.demos.dom followed by rchland.ibm.com.

□ Right click My Computer and then select the Network tab. Join the Domain (in caps) IBMROCHESTERMN0. You might have to sign on as an administrator powered user. This step takes a bit of time.

Lab Cleanup

Please delete all EIM associations and EIM identifiers you created:

□ 1. In iSeries Navigator, click + next to the lab system name: *s400a*
□ 2. Click + next to *Network*.
□ 3. Click + next to *Enterprise Identity Mapping*.
□ 4. Click + next to *Domain Management*.
□ 5. Click + next to *EIM domain for COMMON*.
□ 6. Click + next to *Network*.
□ 7. Open the *Identifiers* list.
□ 8. From the identifiers list page, right click over any identifiers you created and select *Delete*.
□ 9. Click - next to *Network*.

Please delete the QFileSvr.400 folders you created:

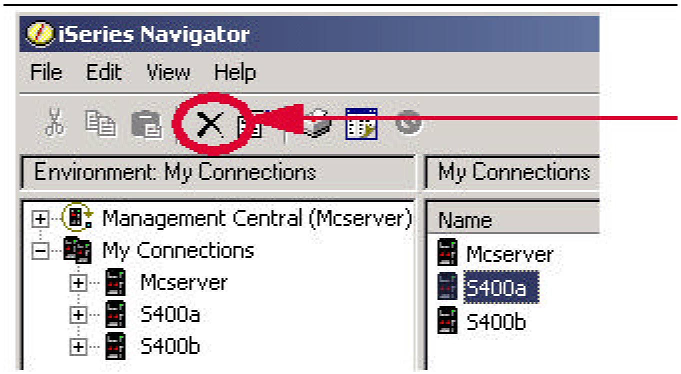
Instructions if you created a folder to get to **s400b** from **s400a**:
□ 10. In iSeries Navigator, click + next to the lab system name: ***s400a***
□ 11. Click + next to *File Systems*.
□ 12. Click + next to *Integrated File System*.
□ 13. Click + next to *QFileSvr.400*.
□ 14. Right click over the folder ***s400b*** and select *Remove*.
□ 15. Click - next to *File Systems*.

Instructions if you created a folder to get to **s400a** from **s400b**:
□ 16. In iSeries Navigator, click + next to the lab system name: ***s400b***
□ 17. Click + next to *File Systems*.
□ 18. Click + next to *Integrated File System*.
□ 19. Click + next to *QFileSvr.400*.
□ 20. Right click over the folder ***s400a*** and select *Remove*.
□ 21. Click - next to *File Systems*.

Please <u>delete</u> the iSeries Navigator connections wsXX created for **s400a** and **s400b**:

NOTE: Only do this when your work station is signed onto wsXX.

☐ 22. Close iSeries Navigator. Left click the iSeries Navigator *file* pull down and select *Close*.
☐ 23. Bring up iSeries Navigator by double clicking on the iSeries Navigator icon on the desktop. On the left, expand *My Connections* by clicking +.
☐ 24. In the My Connection list menu, highlight **s400a** and select the *delete* button from the button bar. The delete button is shown below:



Delete button.

☐ 25. In the My Connection list menu, highlight **s400b** and select the *delete* button from the button bar.
☐ 26. Sign off the work station.