IBM Systems - iSeries

Networking
iSeries support for Windows Network Neighborhood (iSeries NetServer)

Version 5 Release 4

IBM Systems - iSeries

Networking
iSeries support for Windows Network Neighborhood (iSeries NetServer)

Version 5 Release 4

Note

Before using this information and the product it supports, read the information in "Notices," on page 73.

Tenth Edition (February 2006)

This edition applies to i5/OS version 5, release 4, modification 0 (product number 5722-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

Contents

Part 1. iSeries NetServer

iSeries Support for Windows Network Neighborhood (iSeries NetServer™) is an IBM i5/OS™ function that enables Windows 2000, Windows XP, and Windows Server 2003 clients to access i5/OS shared directory paths and shared output queues. Windows clients on a network utilize the file and print sharing functions that are included in their operating systems. You do not need to install any additional software on your PC to use and benefit from iSeries NetServer. However, if you need to administer iSeries NetServer properties from your PC client, you must have iSeries Access for Windows, iSeries Navigator, and i5/OS Host Servers – Option 12 installed.

See the following information for specific information on getting started with and using iSeries NetServer.

Chapter 1. What's new for V5R4

iSeries NetServer has the following performance and scalability enhancements and new functions for V5R4:

- **Threading support:** To increase performance, NetServer now supports the use of pools of threads to process client requests. The new QZLSFILET job handles threaded requests.
- **Opportunistic locks:** Clients have the option of caching application requests to reduce network traffic and server overhead.
- **LAN Manager password hash:** When enabled, it allows Windows clients to authenticate with the less secure (not case sensitive) LAN Manager password hash even if the more secure (case sensitive) NT password hash is also provided and does not match.
- **Message authentication/signing support:** For more secure communications between the client and server, NetServer now supports connection request signing. Signing requests provides improved protection from the following types of attacks: connection hijacking, downgrade attack, rogue server and spoofing by counterfeit servers, active message modification, and replay attacks. See "Require clients to sign requests" on page 54 for more information.
- **Windows-style messages:** The server can be configured to alert users who are running Microsoft Messenger or similar service using the iSeries Navigator graphical user interface (GUI). See Chapter 11, "Use Windows-style messages with iSeries NetServer," on page 55 for more information.

Chapter 2. Printable PDF

To view or download the PDF version of this document, select iSeries NetServer (about 743 KB).

Other information

You can also view or print any of the following PDFs:

- Redbooks:

  The AS/400 NetServer Advantage  describes how to configure and administer iSeries NetServer shares and printers and describes considerations for moving file and print serving from an Integrated Netfinity Server using Warp Server/400 or Novell Netware to iSeries NetServer.

Saving PDF files

To save a PDF file on your workstation for viewing or printing:

1. Right-click the PDF file in your browser (right-click the link above).
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF file.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html)  .

Chapter 3. iSeries NetServer versus iSeries Access for Windows

You do not need to have iSeries Access for Windows or iSeries Navigator installed to use and benefit from iSeries NetServer. Although iSeries NetServer provides specific support for accessing integrated file system and printing resources, it does not provide the same range of tools and interfaces as iSeries Access for Windows .

iSeries NetServer and iSeries Access for Windows differ in the following ways:

iSeries NetServer

- Does not require any proprietary software that is installed on the PC client. The operating system of your PC client contains all of the software that is required to access iSeries NetServer. iSeries NetServer does not require that you install additional software unless you are administering iSeries NetServer functions from a PC client by using iSeries Navigator.
- You can share a directory with read-only access.
- You can hide a share from the network by ending the share name with a $.
- You can hide iSeries NetServer from Windows My Network Places.
- You can share individual directories. This lends to better i5/OS security.

iSeries Access for Windows

- Has additional functions not available in Windows: 5250 emulation and data transfer.

For information on installing iSeries Access for Windows, see "Install iSeries Access for Windows on Windows PCs using iSeries NetServer."

Install iSeries Access for Windows on Windows PCs using iSeries NetServer

You can use iSeries NetServer to easily install iSeries Access for Windows on your Windows client. Remember, administering iSeries NetServer from a PC client requires the use of iSeries Navigator, which is a subcomponent of iSeries Access for Windows. To install iSeries Access for Windows on your Windows client, follow these steps:

For Windows 2000:

1. Open the Windows **Start** menu.
2. Select **Search**.
3. Select **For files or Folders...**
4. Click the **Computers** link.
5. In the **Computer Name** field, specify the server name of iSeries NetServer.
6. Click **Search Now**.
7. Double-click the computer that was found in step 6.
8. Open the **QIBM** folder.
9. Open the **ProdData** folder.
10. Open the **Access** folder.
11. Open the **Windows** folder.
12. Open the **Install** folder.

13. Open the **Image** folder.
14. Double-click **Setup.exe**. The iSeries Access for Windows Install Wizard takes you through the process of installing iSeries Access for Windows on your PC.

    Note: Ensure that you select to have the **Network** option of iSeries Navigator installed.

For Windows XP:

1. Open the Windows **Start** menu.
2. Select **Search**.
3. Click **Computers or People**.
4. Click **A Computer in the Network**.
5. Specify the server name for iSeries NetServer in the appropriate field.
6. Click **Search**.
7. Double-click the computer that was found in step 6.
8. Open the **QIBM** folder.
9. Open the **ProdData** folder.
10. Open the **Access** folder.
11. Open the **Windows** folder.
12. Open the **Install** folder.
13. Open the **Image** folder.
14. Double-click **Setup.exe**. The iSeries Access for Windows Install Wizard takes you through the process of installing iSeries Access for Windows on your PC.

    Note: Ensure that you select to have the **Network** option of iSeries Navigator installed.

For Windows Server 2003:

1. Open the Windows **Start** menu.
2. Select **Search**.
3. Click **Other search options**.
4. Click **Printer, computers, or people**.
5. Click **A computer in the network**.
6. Specify the server name for iSeries NetServer in the appropriate field.
7. Click **Search**.
8. Double-click the computer that was found in step 7.
9. Open the **QIBM** folder.
10. Open the **ProdData** folder.
11. Open the **Access** folder.
12. Open the **Windows** folder.
13. Open the **Install** folder.
14. Open the **Image** folder.
15. Double-click **Setup.exe**. The iSeries Access for Windows Install Wizard takes you through the process of installing iSeries Access for Windows on your PC.

    Note: Ensure that you select to have the **Network** option of iSeries Navigator installed.

iSeries NetServer shares the `QIBM` directory with clients in order to allow i5/OS users who already have user profiles to install iSeries Access for Windows on their PC clients. However, iSeries NetServer does not automatically configure guest support, and users without iSeries user profiles are not able to access

integrated file system directories and output queues using iSeries NetServer. Only the network administrator can remove the file share for the QIBM directory.

To allow guests to have access to shared resources, you must configure the iSeries NetServer Advanced - Next start properties with a user profile for guest or anonymous users.

Chapter 4. Linux and Samba client support

The Linux/Samba client is also supported on iSeries NetServer. This support allows a Linux client running Samba to connect to iSeries NetServer through the smbclient and smbmount client utilities. ASCII printing (text, PDF, and postscript) is supported through the smbclient utility.

The Linux requirement is a kernel version of 2.4.4 or greater and Samba 3.0.9 or greater. Samba is an open-source client and file server that is compatible with Microsoft Networking, which comes with many current distributions of Linux. For more information on Samba, Samba commands, or to download the latest version, see the Samba Web site (www.samba.org)  .

For more information on using Linux/Samba to access iSeries NetServer, see the iSeries NetServer Web site (www.ibm.com/eserver/iseries/netserver/linux.htm)  .

Chapter 5. Get started

iSeries NetServer allows personal computers that run Windows or Linux software to seamlessly access data and printers that are managed by your iSeries server. To begin using iSeries NetServer, follow these steps:

1. **"Requirements"**
   Lists the necessary requirements for using iSeries NetServer.
2. **"Configure iSeries server for NetServer"**
   Provides you with a path for configuring iSeries NetServer.
3. **"Configure and connect your PC Client" on page 14**
   Ensures that you have properly set up your PC operating system to use iSeries NetServer.
4. **"Find iSeries NetServer on the iSeries network" on page 20**
   Ensures that you can access shared resources on the iSeries network.

Requirements

To function properly on iSeries and with network clients, iSeries NetServer requires the following:

- An iSeries server properly connected with Version 4 Release 2 (V4R2) OS/400 or later configured for a TCP/IP network.
- A system name that does not conflict with the system name that iSeries Access for Windows uses. See Server name guidelines for more information.
- An up and running Network Printing Server (NPS) in order to make use of iSeries NetServer print sharing capabilities. See "Configure iSeries server for NetServer" for more information.
- **Client for Microsoft Networks** network component installed on your PC client. Once this component and TCP/IP are installed and configured, you will have access to the integrated file system directories and the iSeries server output queues shared with the network.

  Note: If Linux clients are used, the appropriate Samba support must also be installed.
- The iSeries NetServer server name and Internet Protocol (IP) address resolution strategy. For example, Domain Name System (DNS), Windows Internet Naming Service (WINS), or LMHOSTS file.
- Boss Option 12 (Host Servers), an optional part of the Base OS, needs to be installed for correct iSeries NetServer function.

Configure iSeries server for NetServer

You must have `*IOSYSCFG` special authority to change any part of iSeries NetServer configuration. In addition, you must have `*SECADM` special authority to change the iSeries NetServer guest user profile. These changes will take effect the next time iSeries NetServer is started.

1. Verify that TCP/IP support is configured on your iSeries. You must have at least one external TCP/IP interface configured and active to use iSeries NetServer.
   - Use the Configure TCP/IP (CFGTCP) command to check or change interfaces, routes, setup host table, and domain name services. Once the configuration is complete, use the Start TCP/IP (STRTCP) command to activate the support.
2. Use the Work with Subsystems (WRKSBS) command to confirm that the QSERVER subsystem has started.
3. Verify that the iSeries NetServer server name is unique on the network. To change the iSeries NetServer default server and domain name, use the following command:

   ```
   CALL QZLSCHSN PARM (server-name domain-name
   'text description or comment' X'00000000')
   ```

Once you change the iSeries NetServer server name, you should add it to the Domain Name System (DNS) or your PC client's LMHOST file.

4. Users who require the file and print-sharing capabilities of iSeries NetServer, but do not have an iSeries user profile need a guest user profile. iSeries NetServer does not automatically configure guest support; users without iSeries user profiles will not be able to access iSeries NetServer.

   Note: For iSeries NetServer print support, the Guest User Profile must have a password.
   To change iSeries NetServer guest support, use the following command:

   ```
   CALL QZLSCHSG (guest-user-profile X'00000000')
   ```

5. To stop and start iSeries NetServer, use the following commands:

   ```
   STRTCPSVR *NETSVR
   ENDTCPSVR *NETSVR
   ```

   All configuration changes made to iSeries NetServer, with the exception of share and session administration, do not take effect until you stop and restart the iSeries server. For more information regarding starting and stopping iSeries NetServer, see Start and Stop iSeries NetServer.

6. Use the Work with Active Job (WRKACTJOB) command to verify that there is a QZLSSERVER job running under the QSERVER subsystem. If the QZLSSERVER job is not active, you must restart iSeries NetServer.
7. Use the Work with TCP/IP Network Status (NETSTAT *CNN) command to verify that the following entries appear in the NETSTAT output file. If you cannot find these entries, then you must restart iSeries NetServer.

   ```
   ** netbios>001:27:44 Listen
   ** netbios>000:00:01 *UDP
   ** netbios>000:00:00 *UDP
   ** netbios>000:30:57 Listen
   ** cifs>427:49:42 Listen
   ```

   Note: The `NETSTAT` command output may be many pages long.

8. Use the Work with Active Job (WRKACTJOB) command to ensure that there is a QNPSERVD job active in the QSYSWRK subsystem. If there is no QNPSERVD job, then you must use the Start Host Server (STRHOSTSVR *NETPRT) command to start the Network Print Server (NPS). Starting the NPS ensures that iSeries NetServer print shares function properly.

Configure and connect your PC Client

Configuring your PC client for use with iSeries NetServer ensures that you have properly set up your PC operating system to use iSeries NetServer shared resources. Configuring your PC operating system properly ensures that all supported PC clients can locate iSeries NetServer and use file and print shares. For information on setting up a Linux/Samba client to use iSeries NetServer, see the iSeries NetServer Web site, for the information on Linux/Samba client support

(www.ibm.com/eserver/iseries/netserver/linux.html)  .

Set up a Windows PC client to find iSeries NetServer

iSeries NetServer supports the following Windows clients: Windows 2000; Windows XP; and Windows Server 2003.

Setting up a Windows PC client to find iSeries NetServer allows you to easily access shared resources from your Windows PC client.

You must first ensure that clients can locate iSeries NetServer on the network. If this is not the case, network PC clients can use the Domain Name System (DNS), Windows Internet Naming Service (WINS), or a LMHOSTS file to locate iSeries NetServer.

Note: If iSeries NetServer and your Windows client are in the same workgroup (domain) and in the same subnet (network segment), then no additional setup on the client is necessary. Also no additional setup may be necessary if iSeries NetServer is to be found by IP address only.

Keep in mind that TCP/IP configuration does not require any changes to support iSeries NetServer. However, any PC client that uses iSeries NetServer must be configured with the following items:

- iSeries NetServer UDP broadcasts
  – – An iSeries server that is placed in the same workgroup (domain) and the same subnet (network segment) as the PC client that uses iSeries NetServer UDP broadcasts.

Or, if the iSeries is not placed in the same workgroup and the same subnet as the PC client as stated in the item above, then the PC client must use one of the following to locate the iSeries:

- iSeries NetServer and Domain Name System (DNS) management
  – – The address of a DNS server if you are using DNS to locate and connect to iSeries NetServer.
- iSeries NetServer and Windows Internet Naming Service (WINS) management
  – – The Windows Internet Naming Service (WINS) configuration information if you are using a network WINS server to locate and connect to iSeries NetServer.
- PC Client and LMHOSTS static configuration files
  – – LMHOSTS entries for iSeries NetServer if you are using LMHOSTS files to locate and connect to iSeries NetServer.

iSeries NetServer UDP broadcasts

In many TCP/IP networks, various routers in the network filter out User Datagram Protocol (UDP) broadcast frames. A client on one side of a router cannot find iSeries NetServer because the UDP broadcast cannot cross the router.

Smaller networks that are set up to filter UDP broadcasts should consider using other mechanisms for locating the server. The following methods are alternatives to using the default iSeries NetServer UDP broadcast:

- Make an entry for iSeries NetServer in the network Domain Name System (DNS) database. Using DNS is the easiest way to locate and connect to iSeries NetServer.
- Configure the Windows Internet Naming Service (WINS) for use with iSeries NetServer.
- Create entries for iSeries NetServer in PC client static configuration files (such as LMHOSTS).

Note: If you place all of your iSeries NetServer and PC clients in the same workgroup and the same subnet, then iSeries NetServer appears in Windows 2000, Windows XP, and Windows Server 2003 My Network Places without any additional configuration.

iSeries NetServer and Domain Name System (DNS) management

Connecting your PC Client with DNS

TCP/IP networks can use the Domain Name System (DNS) to map server system names to IP addresses. In a DNS network, an entry tells clients in the network how to map the name of the server to its correct TCP/IP address.

No DNS entry exists for iSeries NetServer regardless of whether you use the default system name for iSeries NetServer or specify a new system name. If you want PC clients to access iSeries NetServer by

using DNS, then you must add the iSeries NetServer server name and IP address to the DNS database on iSeries. Using DNS is generally the easiest way for clients to access iSeries NetServer on a distributed network.

To add a new DNS database entry for iSeries NetServer on the network, you must specify the server name for iSeries NetServer.

Configuring your PC Client with DNS

Configuring DNS entries for both the iSeries server and iSeries NetServer allows PC clients to address iSeries Access for Windows as `SYSTEM1` while addressing iSeries NetServer as `QSYSTEM1`, even though both use the same IP address. This step avoids any potential conflicts in the client operating system.

If you are using DNS, you must also configure your client to use DNS. To configure your client for use with DNS, follow these steps:

For Windows 2000:

1. Open the Windows **Start Menu**.
2. Select **Settings** and then select **Control Panel**.
3. Double-click **Network and Dialup Connections**.
4. Select the **Protocols** tab.
5. Select **Local Area Connection**.
6. Click **Properties...**
7. Select **Internet Protocol (TCP/IP)** and click **Properties**.
8. Click **Advanced**.
9. Click the **DNS** tab.
10. Specify the host name, domain, DNS service search order, and domain suffix search order for DNS.
11. Click **OK**.

For Windows XP:

1. Click the **Start** button to open the **Start menu**.
2. Select **Control Panel**.
3. Click **Network and Internet Connections**.
4. Click **Network Connections**.
5. Select the appropriate connection and click **Change settings of this connection** task.
6. Select **Internet Protocol (TCP/IP)**.
7. Click **Properties**.
8. Click **Advanced**.
9. Select the **DNS** tab.
10. Specify the host name, domain, DNS service search order, and domain suffix search order for DNS.
11. Click **OK**.

For Windows Server 2003:

1. Click the **Start** button to open the **Start menu**.
2. Select **Control Panel**.
3. Click **Network Connections**.
4. Select **Local Area Connection**.
5. Click **Properties...**
6. Select **Internet Protocol (TCP/IP)** and click **Properties**.

7. Click **Advanced**.
8. Click the **DNS** tab.
9. Specify the host name, domain, DNS service search order, and domain suffix search order for DNS.
10. Click **OK**.

iSeries NetServer and Windows Internet Naming Service (WINS) management

Connecting your PC Client with WINS

Windows NT servers and Linux Samba server can provide the Windows Internet Naming Service (WINS), which allows clients to map server system names to their actual TCP/IP addresses. WINS is a dynamic naming service that resolves NetBIOS computer names to IP addresses. Although the iSeries server cannot act as a WINS server, it can act as a WINS proxy. This enables non-WINS clients to obtain name resolution from WINS. A WINS proxy receives broadcasted name requests from non-WINS clients and resolves them by directing queries to a WINS server.

Note: Using WINS Proxy is not a recommended method of resolving computer names to IP addresses.

You can specify an address for a network WINS server on the iSeries NetServer **WINS configuration - Next start** dialog box in iSeries Navigator. You can then configure clients to connect to iSeries NetServer by using the WINS server.

Once you configure your PC clients and iSeries NetServer with WINS addresses, you do not need to perform any additional network configuration. PC clients can now locate and connect to iSeries NetServer by using WINS.

Note: In a complex TCP/IP network, where the iSeries NetServer is configured as a Logon Server, a WINS solution for address resolution is better than DNS because logon clients in separate subnets need to be able to resolve special NetBIOS service names in addition to the configured iSeries NetServer name.

Configuring your PC Client with WINS

If you are using WINS, then you must configure iSeries NetServer with the address of the network WINS server. You then need to configure your client with the iSeries NetServer IP address or the WINS server IP address.

To configure your client for use with WINS, follow these steps:

If you are using WINS, then you must configure iSeries NetServer with the address of the network WINS server. You then need to configure your client with the iSeries NetServer IP address or the WINS server IP address. To configure your client for use with WINS, follow these steps:

For Windows 2000:

1. Open the Windows **Start Menu**.
2. Select **Settings** and then select **Control Panel**.
3. Double-click **Network and Dialup Connections**.
4. Select the **Protocols** tab.
5. Select **Local Area Connection**.
6. Click **Properties...**
7. Select **Internet Protocol (TCP/IP)** and click **Properties**.
8. Click **Advanced**.

9. Click the **WINS** tab.
10. Specify the WINS server IP addresses in the correct search order.
11. Click **OK**.

For Windows XP:

1. Click the **Start** button to open the **Start menu**.
2. Select **Control Panel**.
3. Click **Network and Internet Connections**.
4. Click **Network Connections**.
5. Select the appropriate connection and click **Change settings of this connection** task.
6. Select **Internet Protocol (TCP/IP)**.
7. Click **Properties**.
8. Click **Advanced**.
9. Select the **WINS** tab.
10. Specify the WINS server IP addresses in the correct search order.
11. Click **OK**.

For Windows Server 2003:

1. Click the **Start** button to open the **Start menu**.
2. Select **Control Panel**.
3. Click **Network Connections**.
4. Select **Local Area Connection**.
5. Click **Properties...**
6. Select **Internet Protocol (TCP/IP)** and click **Properties**.
7. Click **Advanced**.
8. Click the **WINS** tab.
9. Specify the WINS server IP addresses in the correct search order.
10. Click **OK**.

Configure iSeries NetServer with the address of the network WINS server

You can configure iSeries NetServer with the address of the network Windows Internet Naming Service (WINS) server by using iSeries Navigator. WINS allows PC clients to connect to and access iSeries NetServer shared resources.

To configure iSeries NetServer with the address of the network WINS server, follow these steps:

1. Open a connection to iSeries Navigator on your iSeries server.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP**.
5. Right-click **iSeries NetServer** and select **Properties**.
6. Select the **WINS Configuration** tab.
7. Click **Next start**.
8. In the **Primary WINS server** field, enter the IP address of the network WINS server. iSeries NetServer uses this WINS server for client connections the next time that you start iSeries NetServer.
9. In the **Secondary WINS server** field, enter the IP address of the secondary network WINS server. iSeries NetServer uses this secondary WINS server for client connections the next time that you start iSeries NetServer.

10. In the **Scope ID** field, enter a text string to serve as the network scope for the WINS server. The WINS server uses this scope ID the next time that you start iSeries NetServer.

    Note: You must configure any PC clients that use iSeries NetServer with the same scope ID that you specify here. WINS also functions properly if you leave this entry for scope ID blank on both iSeries NetServer and any clients.
11. Specify if you would like to enable or disable the iSeries NetServer to act as a WINS proxy.
12. Click **OK** to save your changes.

PC client LMHOSTS static configuration files

Connecting your PC Client with LMHOSTS

PC client operating systems can provide static configuration files that map server system names to TCP/IP addresses. These files are typically more difficult to manage than a solution that involves more centralized control (for example, a DNS or WINS server). This difficulty results because your network administrator must configure each PC client individually. Static configuration files are very useful, however, in large, distributed networks. In this environment, clients and servers exist in different subnets (network segments) and possibly different workgroups (domains). Static configuration files help clients locate servers.

All PC clients supported by iSeries NetServer provide the LMHOSTS file that can map server system names to IP addresses. The LMHOSTS file contains IP addresses and server system names. You can use these files to map the IP address for both the iSeries server and iSeries NetServer for clients. Mapping the IP address for both iSeries and iSeries NetServer allows clients to find the iSeries server and iSeries NetServer in a large, distributed network environment.

You may also add an entry into the LMHOSTS file that points to a LMHOSTS file that is administered centrally on the iSeries server. By pointing all clients to the central file on the iSeries server, you need to maintain only one LMHOSTS file for the network.

You can find more information about LMHOSTS files in the sample LMHOSTS file that is provided with your Windows operating system. Additional information is available in your operating system documentation.

Configuring your PC Client with LMHOSTS

If you are using the LMHOSTS file, then you must configure LMHOSTS with the system name and IP address for iSeries NetServer to ensure client connectivity. To add a preloaded entry to the LMHOSTS file, follow these steps:

1. Go to the \WINNT\system32\drivers\etc directory.
2. Add the following entry to the LMHOSTS file:

   ```
   TCP/IP-address iSeries-NetServer-server-name #PRE
   ```

   For example:

   ```
   10.5.10.1 QNETSERVER #PRE
   ```

   If the iSeries NetServer is a Logon Server:

   ```
   10.5.10.1 QNETSERVER #PRE #DOM:netdomain (netdomain is the domain name that
   the Logon Server services).
   ```

Find iSeries NetServer on the iSeries network

Finding iSeries NetServer on the iSeries network with your PC client allows you to access shared resources on the network. This also ensures that your connection method to iSeries NetServer is up and running. For information on finding iSeries NetServer on the network using Linux/Samba clients, see the Linux/Samba client support information on the iSeries NetServer Web site (http://www.ibm.com/eserver/iseries/netserver/linux.htm).

Find iSeries NetServer from the Windows client

You can use the Windows client to find iSeries NetServer. This allows you to access shared resources from your Windows client.

If iSeries NetServer and your client are in the same workgroup (domain) and in the same subnet (network segment), follow these steps to find iSeries NetServer:

For Windows 2000 and XP:

1. Open **My Network Places**.
2. Double-click **Computers Near Me**.
3. Select the system name of iSeries NetServer on the iSeries server.

For Windows Server 2003:

1. Open **Windows Explorer**.
2. Expand **My Network Places**.
3. Expand **Entire Network**.
4. Expand **Microsoft Windows Network**.
5. Expand the domain or workgroup in which iSeries NetServer is located.
6. Select the system name of iSeries NetServer on the iSeries server.

If the PC client and iSeries NetServer are not in the same workgroup/domain, follow these steps to find iSeries NetServer:

For Windows 2000:

1. Open **My Network Places**.
2. Double-click **Entire Contents**.
3. Click **Show Entire Contents**.
4. Double-click **Microsoft Windows Network**.
5. Open the domain in which iSeries NetServer is located.
6. Select the system name of iSeries NetServer on the iSeries server.

For Windows XP or Windows Server 2003:

1. Open **Windows Explorer**.
2. Expand **My Network Places**.
3. Expand **Entire Network**.
4. Expand **Microsoft Windows Network**.
5. Expand the domain or workgroup in which iSeries NetServer is located.
6. Select the system name of iSeries NetServer on the iSeries server.

Tips:

You can also use **Find Computer** on Windows to locate iSeries NetServer on your network by following these steps:

For Windows 2000:

1. Open the Windows **Start** menu.
2. Select **Search**.
3. Select **For files or Folders...**
4. Click the **Computers** link.
5. In the **Computer Name** field, specify the server name of iSeries NetServer.
6. Click **Search Now**.

For Windows XP:

1. Open the Windows **Start** menu.
2. Select **Search**.
3. Click **Computers or People**.
4. Click **A Computer in the Network**.
5. Specify the server name for iSeries NetServer in the appropriate field.
6. Click **Search**.

For Windows Server 2003:

1. Open the Windows **Start** menu.
2. Click **Search**.
3. Click **Other search options**.
4. Click **Printer, computers, or people**.
5. Click **A computer in the network**.
6. Specify the server name for iSeries NetServer in the appropriate field.
7. Click **Search**.

Windows clients support the addressing of servers by using both fully qualified names as well as Internet Protocol (IP) addresses. The use of fully qualified names and IP addresses allows Windows clients to access data on iSeries NetServer in the absence of other naming mechanisms.

You can use any of the following valid forms when addressing an iSeries server or iSeries NetServer with a Windows client. For example, you could use any of these forms with the **Find Computer** dialog box.

- `qsystem1.mysite.com`
- `system1.mysite.com`
- `1.2.34.123`

These forms also work from a Disk Operating System (DOS) window, as in the following examples:

- `dir \\qsystem1.mysite.com\qca400\*.*`
- `del \\system1.mysite.com\jim.doc`
- `type \\1.2.34.567\scott.txt`

See “Troubleshoot iSeries NetServer location on the network” on page 69 if you have trouble finding iSeries NetServer on the network.

Chapter 6. Administer iSeries NetServer

Administering iSeries NetServer allows you to manage file and print shares and control other iSeries NetServer functions. The iSeries Navigator subcomponent of iSeries Access for Windows provides the administration interface for iSeries NetServer. By default, iSeries NetServer shares the iSeries Access for Windows install directory with the network.

You can install iSeries Access for Windows by accessing the default iSeries NetServer file share, `QIBM`.

Once you have installed iSeries Access for Windows and iSeries Navigator, you are ready to administer iSeries NetServer. Review the following topics for the information you need to effectively manage iSeries NetServer:

iSeries NetServer

"View and configure iSeries NetServer properties" on page 24
Lists the steps you must take to configure iSeries NetServer properties.

"iSeries NetServer support for Kerberos v5 authentication" on page 24
Describes the steps you must take to enable iSeries NetServer support for Kerberos authentication.

"Change the server name of iSeries NetServer" on page 26
Describes why you would need to change the iSeries NetServer system name and specifies what steps you must take to do so.

"Disabled user profiles" on page 27
Describes the conditions that cause the disabling and re-enabling of iSeries user profiles.

"Starting and stopping iSeries NetServer" on page 28
Lists the steps you must take to end all sharing of iSeries resources with iSeries NetServer.

"Specify subsystems for iSeries NetServer" on page 29
Describes the steps you can take to control which subsystems user jobs run in.

"Set the guest user profile for iSeries NetServer" on page 30
Describes how to define what level of authority a guest user profile has to iSeries NetServer.

"View iSeries NetServer status" on page 30
Lists the steps you must take to view the current status of iSeries NetServer.

iSeries NetServer shared objects

"View a list of iSeries NetServer shared objects" on page 31
Defines **shared object** and describes how to view a list of all shared objects iSeries NetServer is currently sharing.

"View and configure iSeries NetServer shared object properties" on page 32
Lists the steps you must take to configure iSeries NetServer shared object properties.

"View shared object status" on page 32
Lists the steps you must take to view the current statistics for a shared object connection to iSeries NetServer.

iSeries NetServer sessions

"View a list of iSeries NetServer sessions" on page 32
Defines **session** and describes how to view a list of active iSeries NetServer sessions.

"View iSeries NetServer session properties" on page 33
Lists the steps you must take to view iSeries NetServer session properties.

"View iSeries NetServer session connection status" on page 33
Lists the steps you must take to view the current statistics for a workstation connection to iSeries NetServer.

"Stop an iSeries NetServer session" on page 34
Lists the steps you must take to stop a client's use of file and print shares on a specific session.

View and configure iSeries NetServer properties

You can access the server attributes for iSeries NetServer through iSeries Navigator, which allows you to view and configure iSeries NetServer properties.

To display iSeries NetServer properties using iSeries Navigator, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to display a list of TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Properties**.

The iSeries Navigator online help provides detailed information about each of the iSeries NetServer dialog boxes.

iSeries NetServer support for Kerberos v5 authentication

iSeries NetServer supports using Kerberos Version 5 (v5) for user authentication. In order to enable iSeries NetServer support for Kerberos v5 authentication, you must first have the "iSeries Navigator Security option" on page 25, Network authentication service, and Enterprise Identity Mapping (EIM) configured on the iSeries server.

Enable support for Kerberos v5 authentication

You are strongly encouraged to use the iSeries NetServer configuration wizard to enable support for Kerberos v5. The configuration wizard helps you configure the necessary services required for use with Kerberos v5. See "iSeries NetServer configuration wizard" on page 25 for instructions on how to start the iSeries NetServer configuration wizard.

You may enable iSeries NetServer support for Kerberos v5 authentication through iSeries NetServer properties. However, you must also complete the "Additional configuration requirements for Kerberos v5 authentication enablement" on page 25.

If you fail to complete all of the configuration requirements, you will be unable to use iSeries NetServer once you restart the server.

1. In iSeries Navigator, expand **Network**> **Servers**> **TCP/IP**.
2. Right-click **iSeries NetServer** and select **Properties**.
3. On the **Security** tab, click the **Next Start** button.
4. On the **Security Next Start** dialog box, select one of the following authentication methods:
   - If you select **Passwords/Network authentication**, clients that do not support Kerberos or clients that do support Kerberos but are not currently participating in a Kerberos realm, use encrypted passwords to authenticate.
   - If you select **Network authentication**, all clients must use Kerberos to authenticate with the server. Therefore, only clients that support Kerberos v5 can connect to iSeries NetServer once this support is enabled. The following Windows clients do not support Kerberos v5:
     - Windows 95
     - Windows 98
     - Windows NT
     - Windows Me

5. Click **OK**.

iSeries Navigator Security option

To install Security, follow these steps:

1. Click **Start**> **Programs**> **IBM iSeries Access for Windows**> **Selective Setup**.
2. Follow the instructions on the screen. On the **Component Selection** dialog box, expand **iSeries Navigator**, then click to place a check mark next to Security.
3. Continue through the rest of Selective Setup.

iSeries NetServer configuration wizard

Additional configuration is required in order to use Kerberos v5 with iSeries NetServer. The configuration wizard will help you through the additional configuration requirements for using Kerberos v5 with iSeries NetServer.

To start the iSeries NetServer configuration wizard, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**> **Servers**.
3. Click **TCP/IP** to display a list of TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Configuration**.
5. Follow the instructions to complete the iSeries NetServer configuration wizard.

Additional configuration requirements for Kerberos v5 authentication enablement

You must complete all of the following steps prior to restarting the iSeries server.

1. The Enterprise Identity Mapping (EIM) and Network authentication service must be configured on the server in order to use Kerberos v5 authentication. **If you currently have EIM and Network authentication services configured, skip this step and proceed to 2.**

   Note: The EIM configuration wizard gives you the option to configure Network authentication service, if it is not currently configured on your server. In this event, you must select to configure the Network authentication service, as it is a required service in order to use Kerberos v5 authentication with iSeries NetServer.

   To configure EIM and Network authentication services complete the following steps:

   a. Open iSeries Navigator and connect to the system you want to work with.
   b. Expand Network.
   c. Right-click Enterprise Identity Mapping and select Configure.
   d. Follow the instructions in the EIM configuration wizard.

   Note: If Network authentication services is not currently configured on the iSeries server, you will be prompted to configure this service during the EIM configuration wizard. You must ensure that you select to add the iSeries NetServer service principals when configuring Network authentication services.
2. With Network authentication service currently configured on your server, you must manually add the service principal names to the keytab.
   a. **For Windows 2000 clients:**

      HOST/<fully qualified name>@<REALM>
      HOST/<qname>@<REALM>
      HOST/<IP Address>@<REALM>

b. **For Windows XP and Windows Server 2003 clients:**

   cifs/<fully qualified name>@<REALM>
   cifs/<qname>@<REALM>
   cifs/<IP Address>@<REALM>

   Keytab entries may be added using the Kerberos Key Tab (QKRBKEYTAB) API. On a command line, use the following command string: `CALL PGM(QKRBKEYTAB) PARM('add' 'HOST/`*qname*` where *qname* is the fully qualified name or the IP address.

3. Additional setup is also required on the Windows 2000 or Windows Server 2003 domain controller that the iSeries NetServer clients use as the Key Distribution Center (KDC).

   Complete the following steps to configure an iSeries NetServer service principal on the Windows KDC:

   a. Install the Support Tools from your Windows server CD.

      Note: Instructions for installing the Support Tools can be found in the Microsoft KB article Q301423 (support.microsoft.com/support/kb/articles/Q301/4/23.ASP) .

   b. Create a new user in the Active Directory.

   c. From a command prompt, use the ktpass.exe support tool to map a service principal to the newly created user. The password used for ktpass should match the password used to create the service principal on the iSeries system. Substituting your own parameters for the items in < >, use the appropriate command call as follows.

      For Windows 2000 clients:
      ```
      ktpass -princ HOST/<iSeriesNetServerName@REALM> -mapuser <new user> -pass <password>
      ```
      For Windows XP or Windows Server 2003 clients:
      ```
      ktpass -princ cifs/<iSeriesNetServerName>@REALM> -mapuser <new user> -pass <password>
      ```

      Note: Only one principal can be mapped to a user. If both HOST/* and cifs/* principals are needed, each must be mapped to a separate Active Directory user.

   d. Repeat steps 3b and 3c if you want to access iSeries NetServer using additional principal names.

Change the server name of iSeries NetServer

The iSeries NetServer server name is the name you use to install the iSeries Access for Windows and to access your iSeries NetServer over the network and the Internet. Under most circumstances, you do not need to change the server name that iSeries NetServer uses on iSeries. Even though you can connect to iSeries NetServer using any server name you choose, you should not change the server name from its default. The name should be the same as your iSeries system name. If, however, you must change the server name, review the naming guidelines before doing so. You can view the iSeries system name in the iSeries network attributes by using the Display Network Attributes (DSPNETA) CL command.

Note: You must have *IOSYSCFG authority to change the iSeries NetServer configuration. The change to the server name does not take effect until the next time that iSeries NetServer is started.

To change the iSeries NetServer server name by using iSeries Navigator, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to retrieve a list of the TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Properties**.
6. On the **General** page, click **Next Start**. In the **Server name** field, specify the name that iSeries NetServer should use.

Server name guidelines

The default name configured for iSeries NetServer is typically not the same as the TCP/IP system name. This is done in order to avoid conflicts with older versions of Client Access (pre-V4R4) that look for the system name. However, you are encouraged to have the iSeries NetServer name configured to be the same as the system name when possible.

Therefore, if you are using iSeries NetServer for the first time or if you have changed the TCP/IP name of your system, you should also change the iSeries NetServer name to match the system name when the following are true:

- No Windows clients in the network are currently using Client Access for Windows 95/NT (pre-V4R4).
- No users currently have network drives or printers mapped to iSeries NetServer shares.

If you have not completed the migration to iSeries Access for Windows for all Windows PCs on your network from a pre-V4R4 version of Client Access, you should keep the iSeries NetServer name different from the system name to avoid inconsistent results for the clients.

If users in your network currently have network drives or printers mapped to iSeries NetServer shares, you should disconnect these mappings before changing the iSeries NetServer name. Otherwise, these mappings fail when automatically trying to reconnect using the older name. You should also update any DOS scripts on the clients that refer to the older iSeries NetServer name.

To avoid making all of these updates simultaneously, you can select the **Allow iSeries NetServer access using iSeries name on the iSeries NetServer** option on the **General Next Start Properties** dialog box before you change the iSeries NetServer name. The next time iSeries NetServer is stopped and restarted, both names will be recognized. The new system name can be used when configuring new Windows clients while the existing clients continue to use (map to) the previous name.

Disabled user profiles

iSeries NetServer uses iSeries user profiles and passwords to allow network administrators to control how users can access data. In addition, an iSeries system value named `QMAXSIGN` specifies how many unauthorized sign-on attempts disable the user profile.

A user profile becomes disabled when the user tries to access iSeries NetServer a specified number of times with an incorrect password. A user profile cannot become completely disabled when connecting to an iSeries with iSeries NetServer. If a user exceeds the maximum number of sign-on attempts the user profile becomes disabled for only iSeries NetServer use. Other types of access, such as a system sign-on, are not prevented.

iSeries NetServer uses the last-changed date on iSeries user profiles to determine if they have changed since becoming disabled. If the last-changed date is newer than the date of becoming disabled, then the user profile becomes enabled again for use with iSeries NetServer.

Notes:

1. The QSYSOPR message queue displays the CPIB682 error message that indicates when an iSeries user profile was disabled for use with iSeries NetServer.
2. Some clients will try a name and password several times without the user being aware of it. For example, if the user's desktop password does not match the iSeries user profile password, the client may try to access the iSeries NetServer several times before displaying the Network Password popup window. When the correct password is supplied, the user profile may already be disabled for iSeries NetServer use on the iSeries. If you encounter this situation, the Maximum sign-on attempts allowed system value, QMAXSIGN, could be increased to accommodate multiple client authentication attempts. To do this, use the **Work with System Values** command: `WRKSYSVAL SYSVAL (QMAXSIGN)`.

Display disabled user profiles

To display the disabled iSeries NetServer users using iSeries Navigator, follow these steps:

1. In iSeries Navigator, connect to an iSeries server.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to view list of TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Open**.
6. Click on **File** in the upper left corner.
7. On the pull-down select **Disabled User IDs**.

Enable a disabled user profile

You can re-enable a user profile that has become disabled. You need *IOSYSCFG and *SECADM authority to use iSeries Navigator to enable a disabled iSeries NetServer user.

There are three ways that you can enable a user profile that has been disabled.

- Use iSeries Navigator:
  1. In iSeries Navigator, connect to an iSeries server.
  2. Expand **Network**.
  3. Expand **Server**.
  4. Click **TCP/IP** to view list of TCP/IP servers available.
  5. Right-click **iSeries NetServer** and select **Open**.
  6. Click on **File** in upper left corner.
  7. On the pull-down menu, select **Disabled User IDs**.
  8. Click a disabled user ID and select **Enable User ID**.
- Change the user profile. Starting the following command re-enables the user profile. You may exit the Change User Profile screen without making any changes to the properties for the user profile.

  ```
  CHGUSRPRF USRPRF(USERNAME)
  ```

  where *USERNAME* is the name of the user profile you want to re-enable.
- Stop and then restart iSeries NetServer.

Starting and stopping iSeries NetServer

Starting iSeries NetServer allows you to immediately begin sharing data and printers with your PC clients. iSeries NetServer starts automatically when TCP/IP is started. If you ever need to restart iSeries NetServer, then follow these steps:

1. Open a connection to iSeries Navigator on your iSeries server.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP**.
5. Right-click **iSeries NetServer** and select **Start**.

A faster method of starting iSeries NetServer using iSeries Access for Windows is:

1. Open a connection to iSeries Navigator on your iSeries server.
2. Expand **File System**.
3. Right-click **File Shares** and select **Open iSeries NetServer**.
4. Right-click **iSeries NetServer** and select **Start**.

If you do not have iSeries Navigator installed, use the following command to start iSeries NetServer:
```
STRTCPSVR *NETSVR
```

Stopping iSeries NetServer allows you to end all sharing of iSeries resources with iSeries NetServer. Stopping and then restarting iSeries NetServer also allows you to change iSeries NetServer configuration.

To stop iSeries NetServer, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to retrieve a list of TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Stop**.

If you do not have iSeries Navigator installed, use the following command to stop iSeries NetServer:
```
ENDTCPSVR *NETSVR
```

Specify subsystems for iSeries NetServer

You can control the subsystems in which user jobs are run. For example, you can create separate subsystems for users or groups of users.

The QSERVER subsystem is still shipped with the same default pre-start job entries. If a client attempts to use a subsystem that does not have pre-start job entries defined, the server then runs in the QSERVER subsystem using batch-immediate jobs. If this occurs, the jobs maintain the same name, but may have a job type of BCI (batch-immediate) instead of PJ (pre-start) when viewed on the Work With Active Jobs (WRKACTJOB) display.

System performance

The ENDTCPSVR command and the QZLSENDS API also take longer to complete when ending iSeries NetServer. These commands take more time to process because all of the jobs associated with the server must be ended when the daemon job is ended.

The connect time may also be slightly longer when batch-immediate jobs are used.

Add prestart jobs to a subsystem description

When you configure clients to run jobs in a different subsystem than QSERVER, you must also add the necessary pre-start jobs to the subsystem description. For example, to add pre-start jobs for QZLSFILE in another subsystem, you would use the following command string (inserting your own subsystem name): `ADDPJE SBSD(`*`SubsystemName`*`) PGM(QSYS/QZLSFILE) USER(QUSER) STRJOBS(*YES) INLJOBS(1) THRESHOLD(1) ADLJOBS(5) JOB(*PGM) JOBD(QSYS/QZLSPJ) MAXUSE(200) WAIT(*YES) POOLID(1) CLS(QSYS/QPWFSERVER *CALC *NONE *CALC)`. Adding pre-start jobs for QZLSFILET is very similar. Substitute `QZLSFILE` with `QZLSFILET` in the above command string and change the following parameters: `ADLJOBS(0)`, `JOBD(QSYS/QZLSPJ)`, and `MAXUSE(1)`.

This command starts 1 prestart job in the subsystem that you configured. This job is used when a new connection is established to iSeries NetServer. For QZLSFILE, when the number of pre-start jobs drops below 1, five more pre-start jobs are started in order to be used by future connections. For QZLSFILET, there is only one job running in a subsystem.

Specify subsystems

To specify the subsystems that iSeries NetServer server jobs run in, follow these steps:

1. In iSeries Navigator, expand **Network**> **Servers**.
2. Click **TCP/IP**.
3. Right-click **iSeries NetServer** and select **Properties**.
4. Click the **Subsystems** tab.
5. Specify the subsystem settings that you want to use.
6. Use the **Help** button to find information on individual fields.
7. Click **OK** when you are finished.

Set the guest user profile for iSeries NetServer

A guest user profile provides a base level of access for clients who do not have a valid iSeries user profile. You can set the user profile that iSeries NetServer uses for guest users through iSeries Navigator. You can also specify what level of authority guests will have to iSeries shared resources using iSeries NetServer. You need *IOSYSCFG and *SECADM to change the guest user profile information. The change to guest user profile does not take place until the next time that iSeries NetServer is started.

To set the guest user profile for iSeries NetServer, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to retrieve a list of TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Properties**.
6. Go to the **Advanced** dialog box and click **Next Start**.
7. In the **Guest User Profile** field, enter the user profile that you want guests to have when using iSeries NetServer.

   Note: If you leave this field blank, then unknown users do not have access to iSeries resources through iSeries NetServer. In addition, the guest user profile that you specify cannot have any special authorities. Guests should have little or no authority on iSeries.

If you have concerns about the security risks a guest user profile may pose to your system, see "iSeries NetServer guest user profiles" on page 54 for more information.

View iSeries NetServer status

You can access the current status of iSeries NetServer through iSeries Navigator. The iSeries NetServer status dialog box contains important statistical information that will help you to effectively administer iSeries NetServer. You can refresh the current statistics for the server, reset all values to 0, or set the time between refresh requests from the iSeries NetServer Status dialog box.

When you set the time, in minutes, between refresh requests to the host for iSeries NetServer status, the timed refresh values are saved so you do not have to refresh each time the NetServer status dialog box is opened.

Note: Timed refresh values are saved for each system, not for each user.

To display iSeries NetServer status by using iSeries Navigator, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to display a list of TCP/IP servers available.

5. Right-click **iSeries NetServer** and select **Status**.

The iSeries Navigator online help provides more details about each field on the iSeries NetServer status dialog box.

View a list of iSeries NetServer shared objects

You can use iSeries NetServer to access shared resources on an iSeries network. These shares consist of the following items, called **shared objects**:

- **File shares**, which share integrated file system directories on iSeries
- **Print shares**, which share iSeries output queues

You can view a list of shared objects from within iSeries Navigator, which allows you to see all of the objects that iSeries is currently sharing with PC clients by using iSeries NetServer.

To view a list of currently shared objects in iSeries Navigator, follow these steps:

1. In iSeries Navigator, expand **Network**.
2. Expand **Servers**.
3. Click **TCP/IP** to view a list of TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Open**.
5. Expand **Shared Objects** to display a list of currently shared objects.

Tip:

You can also display a list of iSeries NetServer shared objects by using Windows clients. To do so, follow these steps:

For Windows 2000:

1. Open the Windows **Start** menu.
2. Select **Search**.
3. Select **For files or Folders...**
4. Click the **Computers** link.
5. In the **Computer Name** field, specify the server name of iSeries NetServer.
6. Click **Search Now**.
7. Open iSeries NetServer by double-clicking the found computer.

For Windows XP:

1. Open the Windows **Start** menu.
2. Select **Search**.
3. Click **Computers or People**.
4. Click **A Computer in the Network**.
5. Specify the server name for iSeries NetServer in the appropriate field.
6. Click **Search**.
7. Open iSeries NetServer by double-clicking the found computer.

For Windows Server 2003:

1. Open the Windows **Start** menu.
2. Select **Search**.
3. Click **Other search objects**.
4. Click **Printer, computers, or people**.

5. Click **A computer in the network**.
6. Specify the server name for iSeries NetServer in the appropriate field.
7. Click **Search**.
8. Open iSeries NetServer by double-clicking the found computer.

Note: You must enroll all users who are working with shared objects from the QDLS file system into the iSeries system distribution directory. Users who are not enrolled in the system distribution directory are not able to access file shares from the QDLS file system. Use the Add Directory Entry (ADDDIRE) CL command to enroll users in the system distribution directory.

View and configure iSeries NetServer shared object properties

You can access the server attributes for iSeries NetServer shared objects through iSeries Navigator, which allows you to display and change the properties of a file or print share. To view the properties for an iSeries NetServer shared object, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to retrieve a list of the TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Open**.
6. Expand **Shared Objects**.
7. Right-click a shared object and select **Properties**.

The iSeries Navigator online help provides detailed information about each of the iSeries NetServer shared object properties dialog box.

View shared object status

You can view the current statistics for a shared object connection to iSeries NetServer through iSeries Navigator. You cannot change or reconfigure shared object statistics because they are records that contain information only.

To display iSeries NetServer shared object status by using iSeries Navigator, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to display a list of TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Open**.
6. Expand **Shared Objects**.
7. Select a shared object.
8. Right-click the session connection and select **Status**.

The iSeries Navigator online help provides more details about iSeries NetServer shared object status.

View a list of iSeries NetServer sessions

iSeries NetServer starts a session whenever a client successfully accesses a shared file or print resource. The session displays the PC client, user name, and session ID.

To view a list of active iSeries NetServer sessions, follow these steps:

1. Open iSeries Navigator and connect to the server that you want to work with.
2. Expand **Network**.

3. Expand **Servers**.
4. Click **TCP/IP** to retrieve a list of the TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Open**.
6. Expand **Sessions** to retrieve a list of active sessions.

View iSeries NetServer session properties

You can view the attributes for an active iSeries NetServer session within iSeries Navigator. This allows you to see the properties of clients that use iSeries shared resources. You cannot change or reconfigure these properties because they are records of client activity that contain information only.

To display the properties for an iSeries NetServer session, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to retrieve a list of the TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Open**.
6. Expand **Sessions**.
7. Right-click a user session and select **Properties**.

iSeries NetServer supports multiple users, including guests, logged on from the same workstation. Information for each session displays the actual user name even if the guest account was used for authentication. As a result, you can see duplicate sessions with the same workstation and user name. Information will be displayed for the following fields:

- Number of connections
- Number of files open
- Number of sessions

Notes:

1. If multiple sessions have been established, they can end when the iSeries NetServer idle time-out value has expired. This occurs regardless of whether or not there are open files for that session.
2. Multiple users could be active from the same workstation. In V5R2, ending a user session ends only the iSeries NetServer file and print activity for that session. However, when the client workstation detects the loss of connectivity for one of the sessions, the client workstation may decide to end them all and optionally establish new sessions.

Note: The iSeries Navigator online help provides detailed information about each of the iSeries NetServer session properties dialog boxes.

View iSeries NetServer session connection status

You can view the current statistics for a workstation session connection to iSeries NetServer through iSeries Navigator. You cannot change or reconfigure the session connection statistics because they are records of client activity that contain information only.

To display iSeries NetServer session connection status by using iSeries Navigator, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to display a list a TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Open**.

6. Expand **Sessions**.
7. Select a session.
8. Right-click the session connection and select **Status**.

The iSeries Navigator online help provides more details about iSeries NetServer session connection status.

Note: iSeries NetServer now supports multiple users, including guests, logged on from the same workstation.

Stop an iSeries NetServer session

iSeries NetServer now supports multiple users, including guests, logged on from the same workstation. You can end single or multiple user sessions on a workstation.

If multiple users are active from the same workstation, ending a user session will end only the iSeries NetServer file and print activity for that session. In addition, ending an active iSeries NetServer session stops the client workstation use of file or print shares on that session. To stop an active session, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to retrieve a list of TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Open**.
6. Expand **Sessions**.
7. Right-click the user sessions and select **Stop**. If more than one session is active on this same workstation, you are given the option of ending multiple user sessions on the workstation.

Note: Stopping the session of a client does not stop the client from reconnecting to the iSeries server and using iSeries NetServer again.

Chapter 7. iSeries NetServer file shares

An iSeries NetServer file share is a directory path that iSeries NetServer shares with clients on the iSeries network. A file share can consist of any integrated file system directory on the iSeries server. You can create, display, configure, and end iSeries NetServer file shares. The following topics provide you with the information that you need to manage file-sharing:

"Create an iSeries NetServer file share"
Describes how to create a new file share by using iSeries Navigator. A file share enables clients to access iSeries resources.

"Control access to iSeries NetServer file shares" on page 36
Describes how you can set access for a file share and lists the steps you must take to do so.

"Stop file sharing" on page 36
Describes the steps you must take to stop file-sharing.

"Access iSeries NetServer file shares with a Windows client" on page 36
Describes how to access file shares with your Windows client.

In general, all integrated file system limitations and considerations apply when accessing shared directories with iSeries NetServer.

See "Case sensitivity of file systems for iSeries NetServer" on page 37 for information about iSeries file systems and case sensitivity.

Create an iSeries NetServer file share

You can share any directory in the iSeries integrated file system with clients in the network by using iSeries NetServer. Creating an iSeries file share allows PC clients to easily access resources on iSeries.

Unlike iSeries Access for Windows, iSeries NetServer does not share the entire integrated file system with the network by default.

To create a new file share by using iSeries Navigator, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to retrieve a list of TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Open**.
6. Right-click **Shared Objects** and select **New** and then **File**.
7. Use the **General Properties** page to configure the new file share with a name, description, access, maximum number of users, and directory path name.
8. Use the **Text Conversion** page to identify which file types will have their contents converted from the iSeries file coded character set ID to the coded character set ID you specify for the share.

Note: The iSeries Navigator online help provides more details about iSeries NetServer file share properties.

Control access to iSeries NetServer file shares

Assigning an access setting for iSeries NetServer file shares through iSeries Navigator allows you to control the level of access that PC clients have to objects in iSeries integrated file system directory paths. If you set the access of a file share to **Read only**, then clients do not have the authority to change a file. If you set the access of a file share to **Read/Write**, then client users can change any files they have authority to in the shared directory paths.

To set the access for an iSeries NetServer file share, follow these steps:

1. Open a connection to iSeries Navigator on your iSeries.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to retrieve a list of the TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Open**.
6. Expand **Shared Objects**.
7. Right-click a file share and select **Properties**.
8. Click the pull-down menu in the **Access** field.
9. Set the file share access to read only by selecting **Read only**. Set the file share access to read/write by selecting **Read/Write**.

Stop file sharing

To stop the sharing of an integrated file system directory, follow these steps:

1. Open a connection to iSeries Navigator on your iSeries.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to retrieve a list of the TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Open**.
6. Expand **Shared Objects**.
7. Right-click a shared file and select **Stop Sharing**.

Note: A file share that is stopped is still available to all clients that are already using the share. A stopped file share is not available for any new client requests. Any attempts to create a new connection to the stopped share will fail.

Access iSeries NetServer file shares with a Windows client

You can use your Windows client to access iSeries file shares with iSeries NetServer.

To access file shares by using Windows, you can either map file shares to logical drives or use Universal Naming Convention (UNC) mapping. You may find it easier, however, to work with logical drive letters as opposed to UNC mapping.

To map an iSeries NetServer file share to a logical drive on your Windows client, follow these steps:

1. Right-click the **Start** button and choose **Explore** to open the Windows Explorer.
2. Open the **Tools** pull-down menu on the Windows Explorer and select **Map network drive**.
3. Select the letter of a free drive for the file share.
4. Enter the name of an iSeries NetServer file share. For example, you could enter the following syntax:
   ```
   \\QSYSTEM1\Sharename
   ```

Note: `QSYSTEM1` is the system name of iSeries NetServer on the iSeries server and `Sharename` is the name of the file share you want to use.

5. Click **OK**.

To use your Windows client to find iSeries NetServer, see "Find iSeries NetServer on the iSeries network" on page 20 for instructions for your specific Windows client.

Case sensitivity of file systems for iSeries NetServer

All iSeries file systems, except for three, are case *insensitive* and do not cause case sensitivity conflicts with supported PC clients.

The following three iSeries file systems, however, are case *sensitive*:

- QOpenSys
- User-Defined File System (UDFS), if specified case-sensitive when created
- Network File System (NFS), depending on which remote file system you access

The case of file names is significant in case-sensitive file systems. The names can consist of both uppercase and lowercase characters. For example, the QOpenSys file system could have three files in it with the following names:

```
NETSERVE.DAT
NetServe.DAT
netserve.DAT
```

These three files have technically different names (because QOpenSys is case-sensitive) and represent three distinct, separate objects on iSeries.

All the PC clients that iSeries NetServer supports are case insensitive. The case of file names is insignificant because all file names are translated automatically into uppercase. For example, from the three example files that are listed above, all the PC clients iSeries NetServer supports would recognize only the following file:

```
NETSERVE.DAT
```

Therefore, iSeries NetServer may not work correctly when using files in case sensitive file systems. This is particularly true when working with case sensitive file systems while you are using a graphical user interface such as the Windows 95 Explorer.

All other iSeries file systems are case insensitive and do not cause case-sensitivity conflicts with supported PC clients.

Chapter 8. iSeries NetServer print shares

You can share any iSeries output queue with PC clients in the network by using iSeries NetServer. Consequently, you can create, display, configure, and end print shares. A print share consists of any iSeries output queue and supports the following spooled file types:

- User ASCII
- Advanced Function Printing
- SNA Character String
- Auto-select

The spooled file type determines how the spooled files are created on your iSeries. If autoselect is not used, the spooled file type must correspond exactly to the output queue destination or you will experience a print error.

Windows support for iSeries NetServer print shares

The following topics provide you with the information that is necessary to manage print-sharing:

"Create an iSeries NetServer print share"
Describes how to create a print share. Creating a print share enables you to give clients access to network printers.

"PC client print device drivers for use with iSeries NetServer print shares" on page 40
Describes how iSeries NetServer acts as a print server and tells you how to access a print device driver.

"Stop print sharing" on page 40
Describes the steps that you must take to stop print-sharing.

"Use iSeries NetServer print shares with Windows 2000, Windows XP, and Windows Server 2003 clients" on page 40
Describes how to access print shares with your Windows 2000, Windows XP, or Windows Server 2003 client.

Create an iSeries NetServer print share

You can share any iSeries output queue with clients in the network by creating an iSeries NetServer print share. Creating an iSeries NetServer print share allows you to give PC clients access to iSeries network printers.

To create a new iSeries NetServer print share by using iSeries Navigator, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click TCP/IP to retrieve a list of the TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Open**.
6. Right-click **Shared Objects** and select **New** and then select **Printer**.
7. Configure the new print share with a name, description, output queue, printer device driver, spooled file type, publishing status, and printer file by using the **General - Properties** dialog box.

The iSeries Navigator online help provides detailed information about the iSeries NetServer print share dialog box.

PC client print device drivers for use with iSeries NetServer print shares

iSeries NetServer acts as a print server that makes the services of the iSeries Network Print Server (NPS) available to PC clients. NPS allows clients with the correct print device drivers to spool print jobs onto iSeries output queues of various spooled file types. These spooled file types include the following:

- User ASCII
- Advanced Function Printing (AFP)
- SNA Character String (SCS)
- Auto-select

You can access AFP and SCS print device drivers for the supported Windows PC clients in either of these ways:

- AFP print device drivers are available for free download from the IBM Printing Systems Company World Wide Web (WWW) site.

  To download AFP device drivers for your PC client go to the IBM Printing Systems Company Web site at: www.printers.ibm.com

  

  .
- You can also find stand-alone AFP and SCS print device drivers in the `Qca400\Win32\Install\Printer` folder. Under the appropriate directory for your client type, you will find the AFP and SCS print device drivers.

Stop print sharing

You can stop print-sharing from within iSeries Navigator by following these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to retrieve a list of the TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Open**.
6. Expand **Shared Objects**.
7. Right-click a shared printer and select **Stop Sharing**.

Use iSeries NetServer print shares with Windows 2000, Windows XP, and Windows Server 2003 clients

You can use your Windows client to access iSeries print shares with iSeries NetServer. To do this, follow these steps:

For Windows 2000, or Windows XP:

1. Open **My Network Places**.
2. Double-click **Computers Near Me**.
3. Select the system name of iSeries NetServer on the iSeries server.
4. Open iSeries NetServer by double-clicking the found computer.
5. Right-click a shared printer and select **Open**.
6. If prompted, select **Yes** to set up the printer on your computer.
7. If prompted, select the appropriate print device driver for the shared printer.

8. Click **Next**.
9. When you have properly set up the shared printer, click **Finish**.

For Windows Server 2003:

1. Open **Windows Explorer**.
2. Expand **My Network Places**.
3. Expand **Entire Network**.
4. Expand **Microsoft Windows Network**.
5. Expand the domain node.
6. Select the system name of iSeries NetServer on the iSeries server.
7. Open iSeries NetServer by double-clicking the found computer.
8. Right-click a shared printer and select **Open**.
9. If prompted, select **Yes** to set up the printer on your computer.
10. If prompted, select the appropriate print device driver for the shared printer.
11. Click **Next**.
12. When you have properly set up the shared printer, click **Finish**.

Chapter 9. iSeries NetServer domain logon support

In an effort to remove the need for a Windows server to handle domain logon services in an SMB domain, iSeries NetServer has been enhanced to provide this support. Windows clients are able to sign on to an iSeries NetServer domain just as they would sign on to an NT domain. Additional advantages of iSeries NetServer providing these services include:

- iSeries as a primary location for user information and domain logon authentication (including home directory and logon scripts)
- Storage and retrieval of Windows user profiles on iSeries, including Desktop, Start Menu, Favorites, and so on
- Storage, retrieval, and maintenance of Windows system policies from the iSeries

iSeries NetServer provides specific services necessary or directly related to logon support. Thus, iSeries NetServer will identify itself as a Primary Domain Controller (PDC) and function as a Domain Master Browser (DMB) if it is configured as a Logon Server, but iSeries NetServer cannot function as a Backup Domain Controller, nor can it dynamically replicate Logon related information to WinNT Domain Controllers. See the following pages for more information:

"iSeries NetServer and client PC configuration"
Describes the PC client configuration requirements needed to take advantage of the Logon Server support.

"Logon server setup" on page 44
Describes the actions taken when iSeries NetServer starts as a Logon Server.

"Logon server home directories" on page 44
Describes how to configure and map to Logon Server home directories.

"Roaming profiles" on page 45
Describes the use of roaming profiles on the network.

"Logon scripts" on page 47
Describes what logon scripts are and how they are used by iSeries NetServer.

"Policy serving" on page 48
Describes policies and policy serving used on iSeries NetServer.

"Browsing support" on page 48
Describes iSeries NetServer behavior as a Logon Server with browse support.

"Tips and techniques" on page 49
Describes various tips and techniques to help you use iSeries NetServer as a Logon Server.

"Troubleshoot the logon server" on page 50
Describes methods for fixing common problems with the logon server.

iSeries NetServer and client PC configuration

iSeries NetServer is configured as a Logon Server from the **Next Start** dialog box selected from the General page of iSeries NetServer properties.

Windows 2000 Professional and Windows XP Professional clients require the installation of the IBM Networks Primary Logon Client (IPLC) product to take advantage of the Logon Server support. This product can be downloaded from the iSeries NetServer web page


(www.ibm.com/eserver/iseries/netserver/primarylogon.htm). This Primary Logon Client overrides the normal Windows logon flows and uses networking APIs that iSeries NetServer supports.

Note: Only install the IBM Networks Primary Logon Client for Windows (IPLC) on Windows workstation installations. Never install it on a PC configured as a server or a terminal server because it will conflict with that type of installation and not allow any user to log on. A PC server does not sign on to another server. Also, remember that iSeries NetServer Domain Logon Support can remove the need for such servers.

Logon server setup

When iSeries NetServer starts up as a Logon server, the following actions are taken in addition to normal startup:

- A check is done for the existence of the NETLOGON share. If this share does not exist, then a directory is created (/QIBM/UserData/OS400/NetServer/NetLogon) and shared as NETLOGON with read-only access. Logon Scripts, system policies, and default user profiles can be placed in this directory.
- iSeries NetServer registers and begins listening on the following TCP/IP NetBIOS names: __MSBROWSE__<01>, domain<1E>, domain<1C>, domain<1B>, domain<1D>, domain server<00>, server<20>

From a Windows DOS prompt, issuing nbtstat -a server_name will list these registered names. If WINS is configured for iSeries NetServer, then these names are also registered with WINS. If there is a conflict (meaning some other computer already holds one of the unique domain names), then only that particular service does not start and CPIB687 (RC=2) message is sent to QSYSOPR describing the conflict. See the iSeries NetServer web page  for more information on this error message.

Logon server home directories

Configuring home directories on the Logon Server

A PC user can be configured to have a home directory and can be collectively backed up and maintained on the server. The Logon Server that authenticates the user determines the location of their home directory. By default, an iSeries Logon Server considers the Home directory path stored in the user profile (on the iSeries server) as the PC client user's home directory too. For example, if user JOE has a home directory configured in his user profile as /home/joe, then this path is treated as a UNC name (Windows 98) for the client and the client's view of this folder would be \\logonServer\home\joe. The /home directory would need to be shared with a share name of HOME in order for a Windows 98 client to map a drive to it.

Mapping a drive to your home directory

Windows 2000 and Windows XP clients using the IPLC will attempt to map a drive to the user's home directory automatically when they log on.

Home Directories on other servers

Sometimes it is desirable to store user home directories on a server other than the Logon Server. This may be the case if a lot of data is normally transferred to and from the home directories (perhaps they are also being used to serve roaming profiles) and the Logon Server is not equipped to handle this extra load and provide responsive Logon support to many clients at the same time. Remote home directories can be configured in the user profile for the iSeries server. The remote home directory is actually a share on a different server and it is specified by the QNTC path to the share. For example, if home directories are to be stored in share HOME on iSeries server DRACO2, then the home directory field for user JOE could be given as /qntc/draco2/home. Alternatively, individual home directories could be shared from DRACO2, in which case the home directory above would be given as /qntc/draco2/joe.

Specifying the QNTC path name here does not imply that the client is going through the QNTC file system on the Logon Server to reach the remote share on the home directory server. The client makes a

separate direct connection to the remote home directory share. The reason why the QNTC path format was chosen is to be consistent across the system since this is stored in the user's profile. This way, other applications running locally on the iSeries server would, in theory, be able to access this same home directory.

Note: Since this configuration also changes the home directory for the local user that signs on to the iSeries system through PC5250, for example, the ramifications of this need to be considered if there is a possibility that the user will sign on directly to the iSeries server configured as a Logon Server.

Roaming profiles

iSeries NetServer configured as a Logon Server is capable of supporting roaming profiles. Roaming profiles store their personal PC configuration (desktop icons, start menu, registry settings, etc.) on a file server in addition to caching them locally. In this way, they can sign on from various computers and always get their same desktop and profile settings. Other names this function is known by include roving users and profile serving.

In many network environments roaming profiles are not necessary because users tend to have their own workstation they always log in from, and the extra time needed to download and save a personal profile when the function is used only rarely may not be justified. However, there are PC environments where users need to move from workstation to workstation, or they have multiple PCs that should be kept synchronized (perhaps a mobile computer in addition to a desk PC). These are ideal cases to make use of roaming profiles.

Another benefit of storing profiles on the server is that they can be made mandatory. For example, a user cannot change their profile if it is mandatory. Thus, mandatory profiles are downloaded from the server at logon, but are not saved back during logoff.

See the following pages for more information:

- "Configuration from Windows 2000 and Windows XP clients"
- "Mandatory profiles" on page 46
- "Roaming profile issues" on page 46

Configuration from Windows 2000 and Windows XP clients

Windows 2000 and Windows XP provide more flexibility with roaming profiles. By default, the client attempts to download the user's roaming profile from the server. If the client does not attempt to do this, you must ensure that the profile is set to Roaming, in order to take advantage of the support.

As a logged-on administrator, use the following steps:

For Windows 2000:

1. Click **Start** and select **Settings**> **Control Panel**.
2. Double click **System**.
3. Click the **User Profiles** tab.
4. Select the user profile and click **Change Type**.

For Windows XP:

1. Click **Start**> **Control Panel**.
2. Double click **Performance and Maintenance**.
3. Double click **System**.
4. Click the **Advanced** tab.
5. In the **User Profile** section, click **Settings**.

6. Select the user profile and click **Change Type**.

You can also copy an existing Windows user profile to the server in order to prime the roaming user profile for a user. From the **User profile** dialog box you opened in the previous steps, click the **Copy to** button. Locally cached profiles (preferences and settings) can be replicated to the Logon Server just like you would copy user folders from \Windows\Profiles for Windows 98. Make sure you are copying the profiles into the folder that the NT clients will load them from. See the next section for discussion on profile locations. If you are migrating multiple profiles from an NT server to an iSeries Logon server, then it will probably be more efficient to copy over the entire \WINNT\Profiles folder.

By default, clients with the IPLC attempt to load or store roaming profiles in the subdirectory, Profiles, of the user's home directory. You can override this behavior by changing the user Profile Path that is configured.

For Windows 2000:

1. Click **Start** and select **Settings**> **Control Panel**.
2. Double click **Administrative Tools**.
3. Double click **Computer Management**.
4. Expand **Local Users and Groups**.
5. Click the **Users** folder to display the list of users.
6. Double click the user and select the **Profile** tab.
7. Specify the profile path.
8. Click **OK**.

For Windows XP:

1. Click **Start** and select **Control Panel**.
2. Double click **Performance and Maintenance**.
3. Double click **Administrative Tools**.
4. Double click **Computer Management**.
5. Double click the user and select the **Profile** tab.
6. Specify the profile path.
7. Click **OK**.

The Profile path is typically specified in the following form: \\logonserver\profilesShare\profileDirectory

Mandatory profiles

Mandatory profiles are roaming profiles that the don't get updated when the user logs off. Even if the user makes changes to their desktop settings while logged on, these changes won't be saved, and they will see the same settings the next time they log on. Windows 98, Windows 2000, and Windows XP clients support the loading of Mandatory profiles.

To change a Windows 2000 or Windows XP profile to be mandatory, open the folder on the Logon server where the profile is stored and change the extension of Ntuser.dat from .dat to .man.

To prevent the user from altering their profile in any fashion, you will also need to ensure the share is configured as read-only and the appropriate integrated file system directory permissions are set.

Roaming profile issues

There are several issues or conflicts that can occur in a roaming profile environment that basically come down to administrative questions.

Most items stored on the desktop or in the Start folder are shortcuts, so if the different PCs that the user is logging on from aren't set up the exact same way (installed programs, folders, etc.) then the shortcuts may not be valid, and you may see a series of invalid shortcut errors when you log on in these situations.

For the same reason as above, it's best not to mix and match different Operating Systems for the same user. Windows 98 and Windows NT profiles can co-exist in the same profile folder on the server; however, because different types of information are stored in each case, you may see inconsistencies; particularly if the profiles are not mandatory.

If the same user is logged on to the same Logon Server from different clients, user profile info is saved independently during logoff for each. So, the last one to log off will reflect the actual changes saved to the profile.

You may see the message, Your roaming profile is not available. You will be logged on with your local profile. This typically means that the roaming profile could not be found in the expected place. See "Configuration from Windows 2000 and Windows XP clients" on page 45 for information on copying a user profile to the server.

The error may also indicate that either the configured roaming profile folder is not shared or the integrated file system directory permissions do not allow access.

Users may, inadvertently or not, store files other than shortcuts on their desktop. If these files are very large, it can significantly slow down the logon process. A workaround is to specify certain profile subfolders not be included in the transfer between Logon Server and client.

Logon scripts

Logon scripts are DOS batch files that the client downloads and runs during the logon process. Logon scripts are placed in the NETLOGON share (by default, the NETLOGON share is /QIBM/UserData/OS400/NetServer/NetLogon for iSeries NetServer) on the Logon Server. Special naming conventions must be followed for an iSeries Logon Server to report logon script file names to the client. The following steps are used by iSeries NetServer to determine the logon script name. Assuming a user name of KRISTY, who is a member of the iSeries Primary Group PCGROUP.

1. If the file KRISTY.BAT (case does not matter for case insensitive file systems) exists in the NETLOGON share, then that file is used as the logon script.
2. Else if PCGROUP.BAT exists in the NETLOGON share, then that is used.
3. Else the file name QZLSDEFT.BAT is used. If that file does not exist or is not accessible, then no logon script is processed.

Notes:

1. Placing a new user or group logon script in the NETLOGON share is not guaranteed to be picked up by the user at the next logon without restarting iSeries NetServer because this item is cached. However, performing a CHGUSRPRF command on a user (with or without options) will cause the cache to be updated during the next access and the new logon script should be found.

If the user is logging on from a PC with the IPLC, that client is limited to DOS 8.3 logon script file names. For example, if the user logging on is Administrator, and it matches a profile on the iSeries called ADMINISTRA (10 char max), then the first logon script file checked for will be ADMINIST.BAT.

Because many more environment variables are defined for Windows 2000 and Windows XP, these platforms are capable of running more flexible logon scripts than the Windows 98 client. For example, from Windows NT with service pack 4, the following environment variables are understood: %Homedrive%, %Homepath%, %Homeshare%, %OS%, %Userdomain%, %Username%, %Logonserver%, and %Processor_level%.

The following is an example of a logon script designed for users logging in from NT clients:

```
echo Logged into domain: %Userdomain%

echo Mapping X drive to personal share...
net use x: %logonserver%\%username%

echo Mapping Y drive to operating system specific share...
net use y: %logonserver%\%OS%

echo Synchronizing PC time with the server
net time %logonserver% /SET
pause
```

Policy serving

Policy serving in an iSeries domain works basically as it would in an NT domain. If the client is configured for Automatic Remote Update, then it should look for the policy file in the NETLOGON share of the Logon Server and apply the relevant policies during logon. This should be the default. Otherwise, Manual Remote Update can be used to load the policy from a different share. This setting can be checked in the following registry key: HKLM\System\CurrentControlSet\Control\Update, value name UpdateMode. A data value of 1 means automatic.

Policies are a batch of changes that are applied to the PC's registry that control and restrict a number of things, including what shows up on the user's Start menu, whether the user can install software, what the desktop looks like, which commands are restricted, and so on. When you edit a policy file, you are making changes based on a template which you select. Windows-specific shipped templates include common.adm, winnt.adm, and windows.adm. Other applications may provide their own templates that allow the restriction of certain functions in the application. For example, iSeries Access provides several.

System policy files are created with the System Policy Editor (SPE), typically found as poledit.exe. The same editor can run on different OS levels, but it is important to understand that policy files created on Windows 98 and Me can be used by Windows 98 and Me (not Windows NT, Windows 2000, or Windows XP) machines and the file should have the name CONFIG.POL. Policy files created on Windows NT, 2000, and XP cannot be used by Windows 98 or Me and must have the name NTCONFIG.POL.

Be very careful when putting system policies into effect. You can easily lock out a function that you did not intend to on a PC, and since policies are applied to the local registry, it will remain locked out until you specifically turn it back on in the policy file so that the change can be picked up during the next logon.

Browsing support

When iSeries NetServer is configured as a Logon Server, it tries to become the Primary Domain Controller (PDC) for the domain. Part of that responsibility is the role of the Master Browser (MB). This includes being the Domain Master Browser (DMB) for the domain and a Local Master Browser (LMB) for the subnet.

Browsers maintain the list of computers for their respective domain and a list of reachable domains. Computers that have SMB resources to share, announce themselves to the local subnet (typically every 12 minutes). The LMB for that domain and subnet listens for these announcements and adds these computers to their browse list. Backup Browsers on the subnet periodically contact the LMB for the most recent list. If the LMB knows who the DMB is, it will periodically announce itself to the DMB, which in turn asks the LMB for its most recent local (same subnet) list to merge with the DMB's own. The LMB will periodically ask the DMB for the complete primary list. In this way, each browser will eventually have a complete list of computers sharing resources for their domain, and the list will be at most 45 minutes old.

Note: For this support to work as intended, the Browsing Interval configuration property should be left as the default 720 seconds.

Tips and techniques

The following tips and techniques help you to effectively use iSeries NetServer as a Logon Server.

Verifying which Logon Server actually validated your logon

Environment variables are available for Windows NT, Windows 2000, and Windows XP, to query this type of information.

Eliminating extra message questions for roaming users logging on from Windows NT, Windows 2000, and Windows XP.

You may see a message similar to one of the following during logon:

- Your locally stored profile is newer than the one stored on the server.
- A slow network connection to the Logon Server has been detected.

Then you are asked if the locally cached profile should be used instead. If you want to eliminate these types of questions and always download the roaming profile on the server for this particular PC, then perform the following to have the cached profile deleted after logoff:

1. Open the registry and go to HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
2. Create a new REG_DWORD item called DeleteRoamingCache.
3. Give the new item a data value of 1.

Note that if the Logon Server is unavailable, this user will be reduced to logging on locally with the Default User profile, if at all.

Backup Logon Servers

iSeries NetServer does not currently offer the concept of a Backup Logon Server that can automatically take over in the unlikely event that the primary server goes down. However, planning a careful replication strategy ahead of time can make this process relatively painless.

1. Choose an iSeries server as a backup server that is not currently configured as the Logon Server for the domain.
2. Back up the critical logon directories that you use to this server: NETLOGON, home, users, etc.
3. Keep the user profiles in sync between the Logon Server and the Backup. Management Central can be used for this.
4. When the Logon Server is down or a switch-over needs to be made, select the Logon Server role option in the NetServer properties of the Backup and restart iSeries NetServer.
5. If not using WINS, update the centrally administered LMHOSTS file if necessary.

Use Browstat.exe to verify domain status

Besides nbtstat, Browstat is also a helpful Microsoft utility that comes with the NT Resource Kit, and Developer Studio subscriptions. It has several functions that iSeries NetServer can support including STATUS, ELECT, GETBLIST, GETMASTER, GETPDC, and VIEW.

Troubleshoot the logon server

Cannot find the Logon Server?

Most likely, the PC message you see are similar to one of the following:

- No domain server was available to validate your password.
- The system could not log you on now because the domain X is not available.

This can occur for a number of reasons:

- The client cannot resolve to the Logon Server. This is the most common reason and there can be a variety of causes, depending how the network is configured. The client PC must be able to get the IP address of the Logon Server based on the domain name. If the client and Logon Server are located on different TCP/IP subnets, then typically broadcast queries are not sent across. There are three solution strategies:
  1. It may just work using the domain discovery support of the Microsoft Browsing protocol/support . The iSeries Browsing support is discussed in a previous section, but the basic idea is that if at least one browser server for the domain exists in the subnet that the PC will log on from, and that LMB has knowledge of the DMB (Domain Master Browser), then the client can ask it for the name of the Logon Server, after which normal name resolution can proceed (DNS, etc.). However, there is not always an LMB available to service these requests, and in that case, one of the following backup solutions should be put in place.
  2. WINS. Windows Internet Name Service is the general solution and recommended for complex TCP/IP networks because computers AND the services they render are matched with IP. It requires at least one WINS server running on a computer with that capability somewhere on the network. Then, each computer needing the service should be configured with the IP address of the WINS server. This configuration is not explained here.
  3. Static LMHOSTS configuration file on the PC. Host lines can be appended with #PRE and #DOM:domain directives to preload domain controllers into the name cache. See the sample files shipped with Windows for more information. Note that LMHOSTS files can include files on servers so that this solution can still be centrally administered.

     Note: The Logon support provided by iSeries NetServer is for clients in the same TCP/IP network segment as the server. If your client is in a different segment or subnet, then these resolution strategies are not guaranteed to work. However, a trick that often works for Windows 2000 or Windows XP clients is to change the workgroup of the client machine to one that is **different** than the domain name assigned to iSeries NetServer.
- iSeries NetServer is not started or it didn't start as a Logon Server for the domain in question. Check that it is configured as a Logon Server and that there are no conflict messages in QSYSOPR. If you see a CPIB687, read the detailed description for more information on the exact nature of the conflict.

User name could not be found

This message normally indicates that the user attempting to log on does not have a user profile on the iSeries Logon Server. A guest user may not sign on to an iSeries domain. In extreme cases where the Logon Server is very busy or slow, the user may not be making it into iSeries NetServer's cache quick enough to respond. If this is the case, attempting the logon again should succeed.

Password incorrect

You are likely to see the following messages when attempting to log on in this situation:

- The domain password you supplied is incorrect or access to the Logon Server has been denied.
- The Logon attempt was unsuccessful. Select Help for possible causes and suggested actions.

Here are the possible causes for these messages and resolutions:

- The password you sign on to the domain with does not match the password in your iSeries user profile. Use your iSeries password and try again.
- The password in your iSeries profile has expired. Unfortunately, you cannot change your iSeries password through Windows, so this must be directly done to your profile.
- Your iSeries user profile is disabled. The administrator must enable it.
- You are disabled for iSeries NetServer access. The iSeries NetServer administrator can check this condition and reenable you from iSeries Navigator.
- Although you are typing the correct password, Windows 98 is using an old cached password. The boot drive on the client PC needs to be scanned for a user.pwl file and then remove this file.
- For Windows 2000 and Windows XP it is possible that the wrong machine is being resolved to. Try prefacing the user name with the domain name in the logon prompt like this: domain\user, where user is the username and domain is the domain name.

For Windows 2000 and Windows XP your password also has to match the password stored in the local profile if you have a local profile. If these do not match, then you will see a message like, The system could not log you on. Your network account and password are correct, but your local account password is out of sync. Contact your administrator.

Cannot find the iSeries NetServer domain through My Network Places.

You have configured iSeries NetServer as a Logon Server for domain X, but X does not show up in the Microsoft Windows Network of domains. Some possibilities are:

- iSeries NetServer failed to come up as the DMB because of a conflict with another computer. Check for message CPIB687 (RC=2) in QSYSOPR.
- iSeries NetServer is not configured for WINS if WINS is in use.
- The client PC is not properly configured for WINS.
- There is no Browser in the local subnet of the PC that is a member of domain X.

Can log on but do not see my home drive mapped for Windows 2000 or Windows XP clients even though the share name exists

The typical problem here is that although the share was created successfully from the client, the path name does not actually exist on the server. When you create a user profile on the iSeries, a default home directory path is put in the profile (/home/user), however, the actual user directory in home is not created automatically. You need to do this manually. For example: ===> CRTDIR '/home/USER1'

I want to use a roaming profile from Windows 2000 or Windows XP, but the option to change it from 'Local' to 'Roaming' is disabled

Remember, that you must be logged onto the target domain with an administrating profile (not the profile you want to change to roaming) in order for the option to be available. In V5R1, iSeries NetServer is able to map longer Windows user names to truncated iSeries profile names. So, you can do the following:

1. Create the user profile ADMINISTRA on the iSeries
2. Give ADMINISTRA a password that matches the password for Administrator on the client
3. Now log onto the iSeries domain with the Administrator profile.
4. Open Control Panel, and then open System.
5. Click on the **User Profiles** tab and make the appropriate changes

My profile is listed as 'Roaming', but changes to my settings (or desktop, etc.) do not get saved

The settings get saved to the locally cached copy of your profile, but they are not being updated on the server. This is readily apparent if you try to log on from a different workstation and you don't see the updates. This problem can occur when the Windows client cannot access the user profile directory where the user profile is to be stored. The following are some things to check:

- Make sure the appropriate access rights are set on each part of the path on the Logon Server.
- Make sure the path is spelled correctly if it is being specified in the User Profile settings on the workstation.
- Also check that unsupported environment variables are not being used. Some environment variables are not active/usable until after logon. For example, if you specify %logonserver%\profiles\%username% as the Profile path in User Manager on a Win NT workstation with a service pack less than 3, then the client will be unable to resolve the %logonserver% environment variable. Try using \\servername\profiles\username instead.
- It's always a good idea to start with a locally cached profile that is copied to the Logon Server.

Locally stored profile is newer than that on the server

This dialog box occurs when you log on and asks you if you want to use your local copy instead. Normally, this is a valid message that you can respond Yes to, so that network traffic is reduced, or this message is received repeatedly after just logging off from the same workstation. Looking at the time stamps on the two profiles, the remote one is 2 seconds older (for example) than the locally cached one which indicates that Windows did a final update to the local profile after it copied it out to the Logon Server. Ensure that the client's time is synched with the server's time.

Incorrect authentication method used

The following message is generally received when a user attempts to log in using a different authentication method than what the server is currently configured to use.

```
There are currently no logon servers available to service the logon request.
```

iSeries NetServer cannot be a Logon Server and have Kerberos authentication enabled as well. This message is typically received when a user attempts to sign onto an iSeries server using a traditional password, when the iSeries NetServer has Kerberos authentication enabled.

Refer to "iSeries NetServer support for Kerberos v5 authentication" on page 24 for information on how to enable Kerberos v5 authentication and traditional password support.

Chapter 10. iSeries NetServer security

Using iSeries NetServer securely ensures that unauthorized users do not have access to iSeries NetServer resources, configuration, or share data. When you take steps to ensure iSeries NetServer security, only authorized users can access iSeries NetServer resources and change iSeries NetServer configuration properties.

You should become familiar with the following topics to ensure the secure use of iSeries NetServer on your network:

"iSeries NetServer user profile authority requirements"
Find out how iSeries user profile authorities are used in securing iSeries NetServer.

"iSeries NetServer guest user profiles" on page 54
Learn how to use guest user profiles with iSeries NetServer.

"Hide iSeries NetServer from the network" on page 54
Know how hiding iSeries NetServer from Windows My Network Places can help keep iSeries NetServer secure.

"Require clients to sign requests" on page 54
Learn how to require request signing in order to protect client/server communications.

iSeries NetServer user profile authority requirements

iSeries NetServer authenticates client file and print requests that are based on the user identity (ID) and password that are used in the Windows desktop logon. If an iSeries user profile matches the Windows desktop client user ID, then the passwords will be checked. If the passwords do not match, iSeries NetServer will prompt the client to enter the correct one.

Note: If the Windows user ID is longer than 10 characters (also the maximum length of the user profile name on the iSeries server), then iSeries NetServer truncates the Windows user ID to 10 characters and attempts to match it with an iSeries user profile. For example, an iSeries user profile called ADMINISTRA could be created to match the Windows Administrator user without requiring guest support.

In order to access iSeries NetServer shared resources, clients may not need an iSeries user profile that matches their Windows desktop user. iSeries NetServer can provide guest support for those clients that need only basic file and print services. This support is not automatically enabled. You can configure it by:

1. Right-click on the iSeries NetServer icon and select **Properties**
2. Select the **Advanced** tab
3. Click the **Next Start** button
4. Specify the guest user profile name in the appropriate field

Note: You need *IOSYSCFG and *SECADM special authority to change the iSeries NetServer guest configuration. Changes take effect the next time iSeries NetServer is started. In addition, the guest user profile should not have any special authorities and should have access only to those iSeries integrated file system directories and output queues that are used for basic file and print services.

iSeries NetServer guest user profiles

iSeries NetServer supports guest user profiles (this is also known as an anonymous user profile). The iSeries server can automatically map an unknown user to the guest user profile if you specify a guest user profile. Your network administrator can specify and change the guest user profile that iSeries NetServer uses, if necessary, on the iSeries NetServer **Advanced - Next start** page within iSeries Navigator. In general, the guest user profile should have very few authorities because the guest user is considered a non-trusted user.

Hide iSeries NetServer from the network

For an added measure of security you can hide iSeries NetServer from the Windows My Network Places.

To hide iSeries NetServer from the network follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to display a list of TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Properties**.
6. Click the **Advanced** tab and click the **Next Start** button.
7. Select **None** in the **Browsing announcement interval** field.

   Note: Setting the browsing announcement interval to **None** stops the host announcements to the network. It also stops domain announcements if iSeries NetServer is configured as a Logon Server and may cause problems for logon services for some networks. In general, the default browsing announcement interval should be left if iSeries NetServer is a Logon Server. The default browsing announcement interval is 720 seconds, or 12 minutes.

Require clients to sign requests

Communications between client and server can be made more secure by requiring clients to sign requests. This is done using a key derived from the client's authentication data. By default, clients are not required to sign requests.

To require clients to sign requests, follow these steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to display a list of TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Properties**.
6. Click the **Security** tab and click the **Next Start** button.
7. From the **Require clients to sign requests** drop down box, choose **Yes**, **Optional**, or **No**.

Chapter 11. Use Windows-style messages with iSeries NetServer

iSeries NetServer can automatically send informational messages to users in the following situations:

- User password is about to expire
- User is denied access for a variety of reasons when trying to connect to a share through iSeries NetServer
- Active users need to be alerted that the administrator is about to stop iSeries NetServer

In order to use the Windows messages with iSeries NetServer, see the following information.

"Configure the clients"
Describes the necessary configuration for PC clients to use the messages.

"Enable the support on iSeries NetServer" on page 56
Describes the steps to take to enable the iSeries NetServer for messages.

"New associated iSeries messages" on page 56
Describes the new text messages added to iSeries NetServer used for clients attempting to connect.

"Display a log of the message send attempts" on page 57
Describes how to use the iSeries NetServer maintenance program to display logged messages.

"Send custom messages through iSeries NetServer" on page 57
Describes how to send customized messages to iSeries NetServer users.

Configure the clients

In order for client workstations to receive these messages, the messenger service must be active. To activate this service, follow these steps.

For Windows 2000 and Windows XP:

1. Click **Start** > **Settings...** > **Control Panel**.
2. Open **Services** from **Administrative Tools**.
3. Scroll down to find Messenger. Ensure that the status is **Started** and the **Startup** type is **Automatic**.

For Windows Server 2003:

1. Click **Start** > **Control Panel**.
2. Open **Services** from **Administrative Tools**.
3. Scroll down to find Messenger. Ensure that the status is **Started** and the **Startup** type is **Automatic**.

Start WinPopup.exe

1. Click **Start** > **Run...**
2. Type *winpopup.exe* in the **Open:** field.
3. Click **OK**.

For Linux:

1. You need to enable Samba's messenger support. Edit the smb.conf file so that it contains a message command directive. The following is an example line:

```
message command = /bin/bash -c 'echo -e WinPopup Message from %f on
$(date): \n >> /tmp/msg.txt; cat %s >> /tmp/msg.txt; echo -e
\n\n >> /tmp/msg.txt; rm %s'
```

2. Restart the Samba server. For example, (on Red Hat): /etc/rc.d/init.d/samba restart.
3. Create a shell script that can read the /tmp/msg.txt file and pop the messages into a window in the background. The following is an example bash script:

```
#!/bin/bash

# Run this script in the background to display a message window where
# WinPopup messages are displayed in sequence. Samba must be started
# and smb.conf must be configured to append messages to /tmp/msg.txt

# remove old messages
rm /tmp/msg.txt
touch /tmp/msg.txt
chmod 666 /tmp/msg.txt

rxvt -fb -sb -fn lucidasanstypewriter-bold-14 -sl 2048 -bg red -fg
white -title SMB Network Messages -geometry 80x10+150+280 -e tail -f
/tmp/msg.txt
```

   Note: This script creates an rxvt window. If you do not have rxvt installed or would rather use an xterm window, substitute xterm instead.
4. Save the script as tailmsg.sh and be sure to make this an executable file.
5. Run this file in the background: ./tailmsg.sh &.

Enable the support on iSeries NetServer

Administrative alerts are turned off by default. To enable Windows-style messaging, perform the following steps:

1. Open iSeries Navigator and connect to the system you want to work with.
2. Expand **Network**.
3. Expand **Servers**.
4. Click **TCP/IP** to display a list of TCP/IP servers available.
5. Right-click **iSeries NetServer** and select **Properties**.
6. Click the **Advanced** tab and click the **Next Start** button.
7. Click the check box next to **Allow administrative alerts**.
8. Specify the **Minimum message severity**. Valid values are 0 to 99.

New associated iSeries messages

The new iSeries messages added to accommodate this support include the following list. These messages are not issued on the iSeries server. Only the text of the messages is used (with replacement) to send as a network message to the client user attempting to connect.

- **CPIB68A**
  CPIB68A: No user profile found for user &1.
- **CPIB68B**
  CPIB68B: The profile for user &1 is disabled.
- **CPIB68C**
  CPIB68C: The password for user &1 is expired.
- **CPIB68D**
  CPIB68D: No password exists for user &1.
- **CPIB68E**
  CPIB68E: User &1 is disabled for iSeries NetServer access.

- **CPIB68F**
  CPIB68F: User &1 was enabled for iSeries NetServer access.
- **CPIB690**
  CPIB690: Password for user &1 will expire in &2 day(s).
- **CPIB691**
  CPIB691: User &1 has successfully connected.
- **CPIB692**
  CPIB692: User &1 encountered Kerberos error &2 connecting through iSeries NetServer.

Note: You must set the minimum message severity value to 10 in order to send the CPIB691 welcome message each time a user connects. Otherwise, the value of 20 to ignores this message. The value of 30 disables information messages CPIB68F, CPIB690, and CPIB691.

Display a log of the message send attempts

At your own risk, you may use the iSeries NetServer maintenance program to display a log of network messages that the server attempted to send. The log contains a maximum of the last 500 messages, by default. These messages are deleted when the log is dumped. You can only see the network messages logged since the last time that they were dumped.

To call the maintenance utility, use the following command.

```
CALL PGM(QZLSMAINT) PARM('32')
```

The log is dumped into a spool file in the QSECOFR output queue. Use the Work with Spooled Files (WRKSPLF QSECOFR) command to display the queue.

Example: Spool file dump of logged messages:

```
TIME               NAME     IP-ADDR   TYPE  RC   MESSAGE

1/23/02 17:39:55  SMBTEST1  C0050939   2     0  CPIB68B: THE PROFILE FOR USER
      SMBTEST1 IS DISABLED.

1/23/02 17:40:16   JOE1     C005095D   7     0  CPIB690: PASSWORD FOR USER JOE1
      WILL EXPIRE IN 3 DAY(S).
```

Note: If the RC column is not 0, then there was either an error delivering the message to the user or the client's message handling service reported an error condition.

Send custom messages through iSeries NetServer

If you have built the GO NETS tools for iSeries NetServer using the QUSRTOOL library support, then you can use the Send NetServer Message (SNDNSVMSG) command to send custom messages to registered users on the network. The command is available through option 14 on the GO NETS menu, and it functions like the NET SEND command on Windows.

The GO NETS tools allow the user to use commands or a menu (instead of the NetServer APIs) to add, change, display, and work with shares, start and end NetServer; and change and display NetServer configuration information.

Example: Send Windows message to user name JOE1 on the network and to user KRISTY specifically on the client machine WORKSTATION1:

```
SNDNSVMSG MSG('Reminder: Memo is due today.') TONETID((JOE1) (KRISTY
WORKSTATION1))
```

Since a workstation name is not provided for the first user (JOE1), the message is sent to the PC that holds the NetBIOS name. Normally, when a Windows 2000, Windows XP, or Windows Server 2003 workstation is started, the workstation registers its NetBIOS name on the local subnet and with WINS (when WINS is configured).

When a user logs on, then the user's name is also registered with the messenger service. To see which names are registered with the messenger service, specify `NBTSTAT -a workstation` from a command prompt. The following example output shows four registered message names on workstation HORSE:

```
        NetBIOS Remote Machine Name Table

      Name                Type            Status
    ---------------------------------------------
    HORSE          <00>  UNIQUE      Registered
    DEPT8          <00>  GROUP       Registered
    HORSE          <20>  UNIQUE      Registered
    DEPT8          <1E>  GROUP       Registered
    HORSE-AFS      <20>  UNIQUE      Registered
    HORSE          <03>  UNIQUE      Registered
    HORSE$         <03>  UNIQUE      Registered
    MANNY          <03>  UNIQUE      Registered
```

Example: Send Windows message to all users with active session connections to iSeries NetServer:

```
SNDNSVMSG MSG('&1, the Hawthorne server will be taken down for a disk
replacement at 1pm') TONETID((*ALLNSVCNN))
```

The `&1` can be used to indicate the user name for replacement text in the message.

Example: Send Windows message to all users who have made a connection in the past to iSeries NetServer (since it was restarted): `SNDNSVMSG MSG('Good morning, dedicated users!') TONETID((*ALLUSERS))`

Messages cannot be longer than 126 character.

Chapter 12. Tips and techniques

You can use the following iSeries NetServer Tips and Techniques to solve problems or to make iSeries NetServer work more efficiently for you:

iSeries NetServer does not appear in Windows My Network Places

iSeries NetServer takes advantage of the Microsoft proprietary browsing protocol which allows it to appear in Windows My Network Places. The Browsing protocol results in a separate list of computers for each protocol on each adapter. As a result, and because iSeries NetServer does not support NetBIOS, the transferring of these lists may result in the loss of non-NetBIOS supporting computers from the list.

It is a good idea to make all the computers in the same subnet members of the same domain (workgroup). This ensures that the browse announcements from iSeries NetServer are received by a computer capable of gathering information for the Windows Network Neighborhood.

Note: If iSeries NetServer is a Logon Server, then it will be the Master Browser for the domain and maintain the list of computers. Again, the browse list may not be complete if there are servers in a different subnet and that subnet does not have its own Master Browser that knows to contact the Domain Master Browser with its list.

iSeries NetServer may also be hidden from the network because of the browse announce interval setting. See "Hide iSeries NetServer from the network" on page 54 for information on how to correct this problem, if this is the case.

iSeries NetServer fails to start

If iSeries NetServer fails to start, you may see the following message in QSYSOPR:

```
Message ID . . . . . :   CPIB683       Severity . . . . . :   40
Message type . . . . . :   Information
Date sent  . . . . . :   04/01/98      Time sent  . . . . . :   14:02:55

Message . . . . :   The iSeries Support for Windows Network Neighborhood
  (NetServer) was unable to start.
Cause . . . . . :   The required iSeries NetServer job QZLSSERVER was unable to
  start because of reason code 5.  See the following reason codes and their
  meanings:
    1 - Unable to retrieve user credentials.
    2 - Unable to retrieve credentials.
    3 - Exchange user profile failed.
    4 - Unable to obtain lock for service program QZLSSRV1 in library QSYS.
    5 - Start of the NetBIOS over TCP/IP failed with return code 3420.
    6 - Start of the internal server failed with return code 3420.
    7 - Error occurred when sharing resources with the network.
```

Use the help information on this message to help you find the cause of the problem.

Start iSeries NetServer at IPL

iSeries NetServer is now automatically started and ended as a TCP server when the Start TCP/IP (STRTCP) or End TCP/IP (ENDTCP) commands are evoked. Additionally, iSeries NetServer can be started and ended as an individual TCP/IP server with the use of the Start TCP/IP Server (STRTCPSVR SERVER(*NETSVR)) and End TCP/IP Server (ENDTCPSVR SERVER(*NETSVR)) commands.

You can specify whether the iSeries NetServer starts automatically when TCP/IP is started by selecting the *Start when TCP/IP is started* option on the **iSeries NetServer General Next Start** dialog box. This value affects TCP/IP start behavior (it is not an iSeries NetServer property), so the changes will not take effect immediately. When using iSeries Navigator in iSeries Access for Windows, you can find this dialog box by:

1. In iSeries Navigator, expand **Network**> **Servers**> **TCP/IP**> **iSeries NetServer**.
2. Right click on the iSeries NetServer icon
3. Select **Properties**
4. Select the **General** tab
5. Press the **Next Start** button

QZLSSERVER job resides in the QSERVER subsystem. The Start Server (QZSLSTRS) and End Server (QZLSENDS) APIs still start and end the server. Because of this, no changes are needed in your start-up program if the QSERVER subsystem is started before TCP/IP is started.

iSeries NetServer security: Guest versus non-Guest

When using iSeries NetServer, normal iSeries user profiles and passwords apply. By default, only users with valid iSeries user profiles and passwords can access resources on the iSeries. Windows 2000, Windows XP, and Windows Server 2003 offer the option to select a different userid. If the passwords do not match, you will see a password window. Windows will optionally remember the password.

An iSeries user profile is disabled from using iSeries NetServer when the user has tried to access iSeries NetServer a number of times with an incorrect password. An iSeries system value name, QMAXSIGN, specifies how many unpermitted access attempts disable a user profile. The Windows operating system will try access again when denied. So it may appear that the QMAXSIGN limit is reached before the number of times actually tried by the client. If the user profile does become disabled for iSeries NetServer, you can use one of several methods to re-enable the user profile. See Enable a disabled user profile for more information.

If a user profile is not found that matches the userid that is used to access iSeries NetServer, you may use an optionally configurable guest user profile. This guest, created by the iSeries administrator who has *SECADM special authority, should only have a password if guest print sharing is being used, and must not have any special authorities. The guest user profile allows iSeries file and print sharing by users who otherwise would not require an iSeries user profile.

Note: The guest user profile must have a password if it is to be used for accessing print shares because the Network Print Server requires one.

Chapter 13. iSeries NetServer API guide

You can access all of the administrative functions that are available through iSeries Navigator by using iSeries application programming interfaces (APIs) . This means that you can administer iSeries NetServer through your CL, COBOL, RPG, C, and C++ programs.

Following is a list of APIs that are currently available for administering iSeries NetServer:

- Add File Server Share (QZLSADFS)
- Add Print Server Share (QZLSADPS)
- Change File Server Share (QZLSCHFS)
- Change Print Server Share (QZLSCHPS)
- Change Server Guest (QZLSCHSG)
- Change Server Information (QZLSSCHSI)
- Change Server Name (QZLSCHSN)
- End Server (QZLSENDS)
- End Server Session (QZLSENSS)
- List Server Information (QZLSLSTI)
- Open List of Server Information (QZLSOLST)
- Remove Server Share (QZLSRMS)
- Start Server (QZLSSTRS)

For additional information about administering iSeries NetServer with APIs, refer to OS/400 APIs.

Chapter 14. Backup and recovery of configuration and share information

iSeries NetServer uses files in the integrated file system to store configuration values and share entries. You should back up these files every time that you save the entire iSeries system and each time you change the administration of iSeries NetServer. In addition, plan the frequency of your save operations carefully to ensure that you always have a usable backup available if your system should fail.

The location of the iSeries NetServer configuration and share data files on the iSeries system is: /QIBM/UserData/OS400/NetServer. The specific files that are needed include:

- **Qazlscfg**: Contains configuration information.
- **Qazlsshr**: Contains share information.
- **Qazlsextxxx**: Contains text conversion information for a file share, where xxx is a file share name.

Note: The following directory should be backed up if iSeries NetServer is configured as a Logon Server: /QIBM/UserData/OS400/NetServer/NetLogon.

For further information on these commands and other useful save and restore options, refer to Backup, Recovery, and Availability.

Chapter 15. Troubleshoot iSeries NetServer

Troubleshooting iSeries NetServer allows you to solve specific problems that are related to your use of iSeries NetServer. You may experience various difficulties when trying to locate iSeries NetServer on the iSeries network or use iSeries NetServer resources. These difficulties may relate to the status of iSeries NetServer on iSeries, the PC client connections, the user profile that you use to operate iSeries NetServer, or other reasons.

The following topics provide you with information on how to troubleshoot the various problems you may encounter while using iSeries NetServer:

"Troubleshoot iSeries NetServer user profile connections"
Learn about what to do if you encounter an error code when trying to access a file share.

"Troubleshoot iSeries NetServer file share directory paths" on page 67
Contains information about directory path problems.

"Troubleshoot iSeries NetServer print share failures" on page 67
Find out what to do to troubleshoot print share problems.

"Troubleshoot print problems when using iSeries NetServer guest support" on page 67
Contains information about guest user problems that may arise.

"Troubleshoot PC client connection problems" on page 67
Learn about how to troubleshoot PC connection problems.

"Troubleshoot iSeries NetServer file share problems" on page 68
Find out what to do to troubleshoot file share problems.

"Troubleshoot print device driver problems" on page 68
Find out what to do if you notice unreadable text.

"Troubleshoot iSeries NetServer using the QSYSOPR message queue" on page 69
Take advantage of the QSYSOPR message queue to solve your iSeries NetServer problems.

"Troubleshoot iSeries NetServer location on the network" on page 69
iSeries NetServer may be difficult to find on the network. Learn about the troubleshooting techniques available to solve this problem.

"Troubleshoot iSeries NetServer using Windows-style messages" on page 69
Find out how Windows-style messages can be used to troubleshoot problems with iSeries NetServer.

Troubleshoot iSeries NetServer user profile connections

When you are trying to access a file share, an error code may appear for any of the following reasons:

Lack of authorization

User profiles may not be authorized to a particular shared directory. If this occurs, ensure that the user can access the directory by using i5/OS control language (CL) commands, such as Work with Object Links (WRKLNK).

Attempting to connect with incorrect password

Users may be unable to use iSeries NetServer if they attempt to connect to iSeries with an incorrect password too many times. If this occurs, then iSeries sends a message (CPIB682) to the QSYSOPR message queue. This message indicates that the user profile has been disabled for iSeries NetServer access. This does not disable the user profile for iSeries or iSeries Access for Windows, but it does stop the user profile from accessing iSeries NetServer.

Note: In V5R1, Management Central has a function to monitor messages from QSYSOPR. An administrator could use this function to be alerted to profiles being disabled for iSeries NetServer use. Also in V5R1, the administrator could use iSeries Navigator to periodically look at a list of disabled users and re-enable users from the panel. To find all disabled user profiles, right-click **iSeries NetServer** and select **Disabled Profiles**.

QZLSFILE and QZLSFILET jobs are not configured for a subsystem

Clients should connect to iSeries NetServer by using their valid user profiles and not the guest user profile. The QZLSFILET or QZLSFILE job might be in the QSERVER subsystem for each active client [user] that connects to an iSeries NetServer [file share]. However, QZLSFILET and QZLSFILE jobs can run in another subsystem if the user has configured other subsystems to run iSeries NetServer jobs. Message CPIAD12 in the job log indicates which user/client the QZLSFILE job is servicing (a QZLSFILET job may have numerous messages in the job log because it services mulitple clients). From iSeries Navigator under **Network** > **Servers** > **TCP/IP**, double-click **iSeries NetServer** and then click **Sessions**. A listing of users and their respective workstation name, logon type, and server session is displayed.

Trying to access a non threadsafe file system while running threaded

A client that is running threaded will receive ″access denied″ type errors when trying to access a non threadsafe file system (such as QDLS or QNetWare). The client will also receive errors when attempting to map a drive to a non threadsafe file system when the client session is running threaded. For a listing of file systems that are not threadsafe, see File system considerations for multithreaded programming in the Multithreaded applications topic.

As of V5R4, iSeries NetServer by default services file shares in a multi-threaded job. The threaded activity for all sessions in a subsystem runs in the pool of threads in the QZLSFILET job for that subsystem. Non threaded client activity is still run in QZLSFILE jobs.

A QZLSFILE job in the correct subsystem is still required to launch a threaded session. Whether a client can run threaded is determined when it first maps a drive to the integrated file system (IFS). The first phase of mapping the first drive for a client runs in a QZLSFILE job. If the session can run threaded, the session is transferred into the single QZLSFILET job in the subsystem. If the file system is not threadsafe, or the ADDEXITPGM THDSAFE() option for the QIBM_QPWFS_FILE_SERV exit point is specified as *UNKNOWN or *NO, or QZLSFILET is not present in the subsystem, the client runs in a QZLSFILE job for this session. The QZLSFILE job log records when a client starts. When a client ends the session, the QZLSFILE job returns to prestart wait status and its job log is cleared. When a client starts a session with a QZLSFILET job, message CPIAD12 is written into its job log. Since the QZLSFILET job is used by multiple client sessions, the session end message, CPIAD13, is written to its job log when a user/client session is ended. These messages will accumulate in the job log.

To prevent ″access denied″ type errors, the recommended solution is to not have the QZLSFILET job started in the QSERVER subsystem (or other user subsystems) . This may involve configuring user subsystems in iSeries Navigator so that some clients run threaded and others non-threaded. Use the following command to remove the prestart job entry for QZLSFILET from the QSERVER subsystem.

```
RMVPJE  SBSD(QSYS/QSERVER)  PGM(QSYS/QZLSFILET)
```

If a prestart job entry is to be removed from a different subsystem, then that subsystem would need to be specified instead of QSERVER along with its correct library (the program would remain the same).

For more information on subsystem configuration, see “Specify subsystems for iSeries NetServer” on page 29.

Active print users

Active print users will have a job in QUSRWRK that connects to iSeries NetServer. A message in the job log indicates to which user the QNPSERVS job belongs.

Troubleshoot iSeries NetServer file share directory paths

You may experience errors when accessing an iSeries NetServer file share if the directory path you have specified does not exist in the iSeries integrated file system.

If you have specified a directory path for a file share, but the directory path does not exist on your iSeries server, then clients will experience an error. The directory path that you specify on the **File Share General-Properties** dialog box must exist on the iSeries server for clients to avoid an error.

Troubleshoot iSeries NetServer print share failures

You may experience trouble when using an iSeries NetServer network printer online for any of the following reasons:

- The network printer may not work online because the user does not have authorization to the iSeries output queue. If this occurs, you should ensure that the user can access the output queue by using i5/OS control language (CL) commands, such as the Edit Object Authority (EDTOBJAUT) command.
- You may experience difficulty with spooling print jobs to an iSeries output queue when using an iSeries NetServer print share. In order for iSeries NetServer print shares to function properly, the Network Print Server (NPS) must be up and running. If you do not start NPS, then iSeries NetServer print shares will not function.
- Clients should connect to iSeries NetServer by using their valid user profiles and not the guest user profile. There is one QNPSERVS job entry in the QUSRWRK subsystem for each active client that connects to an iSeries NetServer print share. The QNPSERVS job starts when a client connects to a shared print resource.
- The guest user profile must have a password and be enabled.
- A maximum of 350 spooled files will be displayed in a network printer window.

Troubleshoot print problems when using iSeries NetServer guest support

When you use the iSeries NetServer guest support to access iSeries output queues, you may experience trouble when trying to access the server. In addition, your specified printer may not go online. If this is the case, you must add a password to the iSeries NetServer guest user profile, SMBGUEST, for example. You must also ensure that you enable the user profile. The Network Print Server (NPS) requires a password for authentication although it will not prompt the user to enter a password.

The addition of a password in the SMBGUEST user profile does not affect users who access iSeries NetServer file and print shares. When a user requires guest support for file and print services, iSeries NetServer does not prompt the user for the SMBGUEST password. Because the SMBGUEST user profile has a password and is enabled, set the initial menu parameter to *SIGNOFF, INLMNU(*SIGNOFF), to deny signon access.

Troubleshoot PC client connection problems

You can test whether your connection method to iSeries NetServer (for example, DNS) is up and running if you experience connection problems. To do so, follow these steps:

1. Open a DOS window from your PC client.
2. Enter the PING command to test your client connection to iSeries. For example, you could PING iSeries NetServer by entering this command:

   ```
   ping QSYSTEM1
   ```

Note: QSYSTEM1 is the server name of iSeries NetServer on iSeries.

If you get a positive return value, then the client connection to iSeries NetServer is operating normally. This means that the method the client uses to connect to iSeries NetServer and iSeries is up and running.

Tip:

Run **nbtstat -A ip-address-of-server** from a command prompt on the client to check connectivity: C:\WINDOWS>nbtstat -a qnetserver. Using nbtstat can also be helpful with connectivity information in case the name of the server is unknown or cannot be resolved.

Another way to check client connectivity to iSeries is to see if there is an active NetServer session for the client. Using iSeries Navigator under **Network** > **Servers** > **TCP/IP**, double-click **iSeries NetServer** and then click **Sessions**. A listing of users and their respective workstation name, logon type, and server session is displayed.

Troubleshoot iSeries NetServer file share problems

If you experience problems with iSeries NetServer file share readiness on iSeries, then you should check the status of iSeries NetServer on iSeries. To do so, follow these steps:

1. Verify that iSeries has started the QSERVER subsystem. If iSeries has not already started the QSERVER subsystem, then start it by using the Start Subsystem (STRSBS) CL command.
2. Verify that iSeries has started the QZLSSERVER job within QSERVER. If iSeries has not already started the QZLSSERVER job, then start it by using the STRTCPSVR *NETSVR CL command.
3. Verify that the QZLSFILE prestarted job is waiting for a program start request (PSRW status on the Work with Active Jobs screen). If threaded support is desired, verify that the QZLSFILET job is awaiting client requests for file or print serving (TIMW or TIMA status on the Work with Active Jobs screen). If neither the QZLSFILET nor a QZLSFILE prestarted job is waiting for a program start request, then use the Start Prestart Jobs (STRPJ) CL command. This starts the prestarted job.

   Note: If a subsystem is configured to start the QZLSFILET job, that single QZLSFILET job services multiple clients and their respective thread-safe file shares. There are multiple QZLSFILE jobs in a subsystem and each one supports one client and all of the non thread-safe file shares that are accessed by a Windows client when using iSeries NetServer. However, if not running threaded, Linux connects to a separate QZLSFILE job for each mount of an iSeries NetServer share.
4. Add the QZLSFILET or QZLSFILE prestarted job to the QSERVER subsystem description (or a different subsystem description if you have configured others) if it is not already present. You can use the Add Prestarted Job Entry (ADDPJE) CL command to add the prestarted job entry.

For more information on threaded client activity and problems that may be encountered, see "Troubleshoot iSeries NetServer user profile connections" on page 65.

Troubleshoot print device driver problems

You may notice unreadable printed text when using the Advanced Function Printing (AFP) print device drivers that you download from the IBM Printing Systems Company web site. The unreadable text occurs because the AFP print device driver substitutes fonts when using information that is directly embedded into the print stream of your print job. There are two options available for you to solve the problem:

1. Turn off **Font Substitution** and turn on **Create Inline Form Definition** in the printer properties on your PC.
2. Install License Program AFP Fonts 5769FN1 and AFP DBCS Fonts 5769FNT on your iSeries.

For more information about installing License Programs, see the Software Installation book.  .

Troubleshoot iSeries NetServer using the QSYSOPR message queue

The system operator's message queue, QSYSOPR, is a good place to look for information about iSeries NetServer. Messages are logged to the QSYSOPR message queue each time that iSeries NetServer starts and stops and when there are any specific errors to report.

The first message indicates whether iSeries NetServer initialized completely during startup. This message is important because it not only specifies whether iSeries NetServer started properly, but it also lists the iSeries NetServer server name.

If iSeries NetServer fails to start successfully, the QSYSOPR message queue logs an error message that indicates the reason for the failure.

Using Display Log (DSPLOG) to find iSeries NetServer

The Display Log (DSPLOG) CL command with parameter MSGID(CPIB680) displays a message that indicates when iSeries NetServer started. The message also specifies the iSeries NetServer server name. You may need to adjust the beginning date of the search by using the PERIOD parameter. The message should read as follows:

```
iSeries Support for Windows Network Neighborhood (iSeries NetServer)
SERVER_NAME Initialization Complete
```

Troubleshoot iSeries NetServer location on the network

If you experience problems when trying to find iSeries NetServer on the network, you can take several steps to resolve the problems:

1. Ping the iSeries NetServer server name. Pinging the iSeries NetServer server name reloads the iSeries NetServer IP address into the PC client cache file.
2. Verify that you are using the correct system name for iSeries NetServer. The QSYSOPR message queue specifies the correct iSeries NetServer server name.
3. Verify that you have configured your PC client to properly resolve the iSeries NetServer server name to an Internet Protocol (IP) address. Configure your PC client to resolve the iSeries NetServer server name to an IP address in one of the following ways:
   - Map the iSeries NetServer server name to its IP address by using the Domain Name System (DNS).
   - Map the iSeries NetServer server name to its IP address by using the Windows Internet Naming Service (WINS).
   - Map the iSeries NetServer server name to its IP address by adding an entry to the LMHOSTS file.

Troubleshoot iSeries NetServer using Windows-style messages

A user trying to connect to a share through iSeries NetServer may be denied access for variety of reasons, including:

- A password mismatch
- Not enough authority to the underlying file system object
- The user profile does not exist
- The user profile is disabled
- The user is disabled for iSeries NetServer access
- The password is expired
- The user profile does not have a password
- There was a Kerberos authentication failure

In each of the previous situations, the client typically does not report a meaningful error message to help distinguish the problem. In V5R2, support has been added to iSeries NetServer to allow Windows-style informational messages to be sent over the network to client users on Windows 2000 and Windows XP, as well as Linux operating systems. This can greatly improve problem analysis for user profile connectivity issues.

For more detailed information using these messages, see Chapter 11, “Use Windows-style messages with iSeries NetServer,” on page 55.

Part 2. Appendixes

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Advanced Function Printing
AFP
AS/400
IBM
iSeries
Netfinity
Operating System/400
OS/400
Redbooks

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Terms and conditions

Permissions for the use of these Publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these Publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these Publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these Publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these Publications, or reproduce, distribute or display these Publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the Publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the Publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED ″AS-IS″ AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Printed in USA