System i

Networking
iSeries NetServer

Version 5 Release 4

System i

Networking
iSeries NetServer

Version 5 Release 4

Note

Before using this information and the product it supports, read the information in “Notices,” on page 55.

Eleventh Edition (January 2007)

This edition applies to version 5, release 4, modification 0 of IBM i5/OS (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

iSeries NetServer

iSeries™ Support for Windows® Network Neighborhood (iSeries NetServer™) is an IBM® i5/OS® function that enables Windows 2000, Windows XP, Windows Server 2003, and Windows Vista clients to access i5/OS shared directory paths and shared output queues.

Windows clients on a network use 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 client 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.

Note: By using the code examples, you agree to the terms of the Code license and disclaimer information.

What's new for V5R4

This topic highlights the changes made to the iSeries NetServer topic collection for V5R4.

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

- **Threading support**

  To increase performance, iSeries 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, iSeries NetServer now supports connection request signing. Signing requests provide 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 "Requiring clients to sign requests" on page 41 for more information.
- **Windows messenger service**

  The system can be configured to alert users who are running Microsoft® Messenger or similar service using the iSeries Navigator graphical user interface (GUI).

What's new as of 31 January 2007

iSeries NetServer enables Windows Vista clients to access i5/OS shared directory paths and shared output queues.

How to see what's new or changed

To help you see where technical changes have been made, this information uses:

- The » image to mark where new or changed information begins.
- The « image to mark where new or changed information ends.

To find other information about what's new or changed this release, see the Memo to users.

Related concepts

"Using Windows messenger service with iSeries NetServer" on page 41
iSeries NetServer can automatically send informational messages to users in some situations.

Printable PDFs

Use this to view and print PDF of this information.

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

Other information

You can also view or print the following IBM redbook™ PDF:

The AS/400® NetServer Advantage  describes how to configure and administer iSeries NetServer shares and printers. It also 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 on your workstation for viewing or printing:

1. Right-click the PDF 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.
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)  .

iSeries NetServer versus iSeries Access for Windows

You do not need to install iSeries Access for Windows or iSeries Navigator to use 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 does.

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

iSeries NetServer

- You do not need to install software on your PC client to use iSeries NetServer. 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

- iSeries Access for Windows provides additional functions: 5250 emulation and data transfer.

Installing iSeries Access for Windows on Windows PCs

You can install iSeries Access for Windows on your Windows client by using iSeries NetServer.

Note: Administering iSeries NetServer from a PC client requires the use of iSeries Navigator, which is a component of iSeries Access for Windows.

iSeries NetServer shares the `QIBM` directory with clients 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 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 from 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.

Installing iSeries Access for Windows on Windows 2000

Here are the steps for installing iSeries Access for Windows on your Windows 2000 client by using iSeries NetServer.

To install iSeries Access for Windows on your Windows 2000 client, follow these steps:

1. Click the **Start** button to open the **Start menu**.
2. Select **Search**.
3. Select **For files or Folders**.
4. Click the **Computers** link.
5. In the **Computer Name** field, specify the iSeries NetServer server name.
6. Click **Search Now**.
7. Double-click the computer that was found in step 6.
8. Expand **QIBM** → **ProdData** → **Access** → **Windows** → **Install**.
9. 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: Make sure that you install the **Network** option of iSeries Navigator.

Installing iSeries Access for Windows on Windows XP

Here are the steps for installing iSeries Access for Windows on your Windows XP client by using iSeries NetServer.

To install iSeries Access for Windows on your Windows XP client, follow these steps:

1. Click the **Start** button to open the **Start menu**.
2. Select **Search**.
3. Click **Computers or People**.
4. Click **A Computer in the Network**.
5. In the **Computer Name** field, specify the iSeries NetServer server name.
6. Click **Search**.
7. Double-click the computer that was found in step 6.
8. Expand **QIBM** → **ProdData** → **Access** → **Windows** → **Install** → **Image**.
9. 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: Make sure that you install the **Network** option of iSeries Navigator.

Installing iSeries Access for Windows on Windows Server 2003

Here are the steps for installing iSeries Access for Windows on Windows Server 2003 client by using iSeries NetServer.

To install iSeries Access for Windows on your Windows Server 2003 client, follow these steps:

1. Click the **Start** button to open the **Start menu**.
2. Select **Search**.
3. Click **Other search options**.
4. Click **Printer, computers, or people**.
5. Click **A computer in the network**.
6. In the **Computer Name** field, specify the iSeries NetServer server name.
7. Click **Search**.
8. Double-click the computer that was found in step 7.
9. Expand **QIBM** → **ProdData** → **Access** → **Windows** → **Install** → **Image**.
10. 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: Make sure that you install the **Network** option of iSeries Navigator.

Installing iSeries Access for Windows on Windows Vista

Here are the steps for installing iSeries Access for Windows on your Windows Vista client by using iSeries NetServer.

To install iSeries Access for Windows on your Windows Vista client, follow these steps:

1. Click the **Start** button to open the **Start menu**.
2. In the **Start Search** field, specify the iSeries NetServer server name.
3. Press Enter.
4. Double-click the computer that was found in step 3.
5. Expand **QIBM** → **ProdData** → **Access** → **Windows** → **Install**.
6. 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: Make sure that you install the **Network** option of iSeries Navigator.

Accessing iSeries NetServer with Linux and Samba client support

If you are using a Linux® client, you can use Samba to access iSeries NetServer.

iSeries NetServer also supports the Linux/Samba client. 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 about Samba, Samba commands, or to download the latest version, see the Samba Web site (www.samba.org).

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

Getting started with iSeries NetServer

With iSeries NetServer, personal computers that run Windows or Linux software can seamlessly access data and printers that are managed by your i5/OS operating system.

Requirements for using iSeries NetServer

To make iSeries NetServer function properly on the i5/OS operating system and with network clients, some prerequisites need to be fulfilled.

Here are the requirements for using iSeries NetServer:

- A System i™ product with the i5/OS or Operating System/400® V4R2, or later, operating system must be installed and configured for a TCP/IP network.
- A system name does not conflict with the system name that iSeries Access for Windows uses. See Server name guidelines for more information.
- You need a running network printing server to use iSeries NetServer print sharing capabilities. See "Configuring i5/OS for NetServer" for more information.
- The client for Microsoft Networks network component must be installed on your PC client. After this component and TCP/IP are installed and configured, you have access to the integrated file system directories and the i5/OS output queues that are shared with the network.

  Note: If Linux clients are used, the appropriate Samba support must also be installed.
- An iSeries NetServer server name and Internet Protocol (IP) address resolution strategy must be used: for example, Domain Name System (DNS), Windows Internet Naming Service (WINS), or LMHOSTS file.
- i5/OS Option 12 (Host Servers), a feature of the operating system, must be installed for iSeries NetServer functions to work correctly.

Configuring i5/OS for NetServer

To verify whether iSeries NetServer is properly configured, you can use a series of commands.

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.

To configure the i5/OS operating system for iSeries NetServer, follow these steps:

1. Verify that TCP/IP support is configured on your i5/OS operating system. You can use the Configure TCP/IP (CFGTCP) command to work with interfaces, routes, host table entries, and domain services. After the configuration is complete, use the Start TCP/IP (STRTCP) command to activate the support.

   Note: You must have at least one external TCP/IP interface configured and active to use iSeries NetServer.
2. Use the Work with Subsystems (WRKSBS) command to confirm that the QSERVER subsystem has started.
3. Verify that the iSeries NetServer system name is unique on the network. To change the iSeries NetServer default system and domain name, use the following command:

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

   After you change the iSeries NetServer server name, you should add it to the Domain Name System (DNS) or to your PC client's LMHOST file.
4. To change iSeries NetServer guest support, use the following command:

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

Users who require the file and print-sharing capabilities of iSeries NetServer but do not have an i5/OS user profile need a guest user profile. iSeries NetServer does not automatically configure guest support. A user without an i5/OS user profile will not be able to access iSeries NetServer.

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

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

   Note: 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 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, 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 might 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. Starting the network print server ensures that iSeries NetServer print shares function properly.

Related tasks

"Starting and stopping iSeries NetServer" on page 20
Starting iSeries NetServer allows you to immediately begin sharing data and printers with your PC clients, while stopping iSeries NetServer ends all sharing of resources. Stopping and then restarting iSeries NetServer also allows you to change iSeries NetServer configuration.

Configuring and connecting your PC client

Configuring your client properly ensures that all supported PC clients can locate iSeries NetServer and use file and print shares.

For information about setting up a Linux/Samba client to use iSeries NetServer, see the iSeries NetServer Web site, for the information about iSeries NetServer Linux Client (Samba) Support .

Setting up a Windows PC client to find iSeries NetServer

iSeries NetServer supports Windows 2000, Windows XP, Windows Server 2003, and Windows Vista.

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 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 needed. If you find iSeries NetServer only by the IP address, then no additional setup is needed.

If iSeries NetServer is not placed in the same workgroup and the same subnet as the PC client, the PC client must use one of the following approaches to locate iSeries NetServer:

- 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.
- iSeries NetServer is configured to register with Windows Internet Naming Service (WINS).
- Create entries for iSeries NetServer in PC client static configuration files (such as `LMHOSTS`).

Related information

iSeries NetServer Linux Client (Samba) Support

iSeries NetServer User Datagram Protocol broadcasts

A system that is placed in the same workgroup (domain) and the same subnet (network segment) as the PC client uses iSeries NetServer User Datagram Protocol (UDP) broadcasts.

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

When setting up smaller networks to filter UDP broadcasts, you should consider using other mechanisms for locating the system.

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 My Network Places of Windows 2000, Windows XP, Windows Server 2003, and Windows Vista without any additional configuration.

Related tasks

"iSeries NetServer and Domain Name System management"
If you are using Domain Name System (DNS) to locate and connect to iSeries NetServer, you need to connect and configure your PC client with DNS first.

"iSeries NetServer and Windows Internet Naming Service management" on page 9
If you are using Windows Internet Naming Service (WINS) to locate and connect to iSeries NetServer, connect and configure your PC client with WINS first.

"PC client LMHOSTS static configuration files" on page 12
In large distributed networks, LMHOSTS static configuration files are helpful for mapping system names to IP addresses.

iSeries NetServer and Domain Name System management

If you are using Domain Name System (DNS) to locate and connect to iSeries NetServer, you need to connect and configure your PC client with DNS first.

Related concepts

"iSeries NetServer User Datagram Protocol broadcasts"
A system that is placed in the same workgroup (domain) and the same subnet (network segment) as the PC client uses iSeries NetServer User Datagram Protocol (UDP) broadcasts.

Connecting your PC client with DNS:

TCP/IP networks can use Domain Name System (DNS) to map system names to IP addresses.

In a DNS network, an entry tells clients in the network how to map the system name to its correct TCP/IP address.

If you want PC clients to access iSeries NetServer by using DNS, then you must add the iSeries NetServer system name and IP address to the DNS database on the i5/OS operating system. 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 iSeries NetServer server name.

Configuring your PC client with DNS:

To avoid any potential conflicts in the client operating system, configure Domain Name System (DNS) entries for both the i5/OS operating system and iSeries NetServer.

Configuring Domain Name System (DNS) entries for both the i5/OS operating system 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.

Configuring your PC client with DNS on Windows 2000:

Here are the steps for configuring your PC client with Domain Name System (DNS) on Windows 2000.

To configure your PC client with DNS on Windows 2000, follow these steps:

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**.

Configuring your PC client with DNS on Windows XP:

Here are the steps for configuring your PC client with DNS on Windows XP.

To configure your PC client with DNS on Windows XP, follow these steps:

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**.
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**.

Configuring your PC client with DNS on Windows Server 2003:

Here are the steps for configuring your PC client with Domain Name System (DNS) on Windows Server 2003.

To configure your PC client with DNS on Windows Server 2003, follow these steps:

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

Configuring your PC client with DNS on Windows Vista:

Here are the steps for configuring your PC client with DNS on Windows Vista.

To configure your PC client with DNS on Windows Vista, follow these steps:

1. Click the **Start** button to open the **Start menu**.
2. Select **Control Panel**.
3. Click **Network and Internet**.
4. Click **Network and Sharing Center**.
5. Click **View status**.
6. Click **Properties**.
7. Select **Internet Protocol Version 4 (TCP/IP 4)** or **Internet Protocol Version 6 (TCP/IP 6)**.
8. Click **Properties**.
9. Click **Advanced**.
10. Select the **DNS** tab.
11. Specify the host name, domain, DNS service search order, and domain suffix search order for DNS.
12. Click **OK**.

iSeries NetServer and Windows Internet Naming Service management

If you are using Windows Internet Naming Service (WINS) to locate and connect to iSeries NetServer, connect and configure your PC client with WINS first.

Related concepts

"iSeries NetServer User Datagram Protocol broadcasts" on page 7
A system that is placed in the same workgroup (domain) and the same subnet (network segment) as the PC client uses iSeries NetServer User Datagram Protocol (UDP) broadcasts.

Connecting your PC client with WINS:

Windows Internet Naming Service (WINS) allows clients to map system names to their actual TCP/IP addresses.

Windows NT® systems and Linux Samba servers can provide WINS, which allows clients to map system names to their actual TCP/IP addresses. WINS is a dynamic naming service that resolves NetBIOS computer names to IP addresses. Although the i5/OS operating system 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. Then you can configure clients to connect to iSeries NetServer by using the WINS server.

After 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:

When using WINS, you must configure iSeries NetServer with the IP address of the WINS and you also need to configure the client to use the same WINS IP address.

Configuring your PC client with WINS on Windows 2000:

Here are the steps for configuring your PC client for use with WINS on Windows 2000.

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

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**.

Configuring your PC client with WINS on Windows XP:

Here are the steps for configuring your client for use with WINS on Windows XP.

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

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. Click **Properties**.

7. Select **Internet Protocol (TCP/IP)** and 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**.

Configuring your PC client with WINS on Windows Server 2003:

Here are the steps for configuring your client for use with WINS on Windows Server 2003.

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

Configuring your PC client with WINS on Windows Vista:

Here are the steps for configuring your PC client for use with WINS on Windows Vista.

To configure your client for use with WINS, follow these steps:
1. Click the **Start** button to open the **Start menu**.
2. Select **Control Panel**.
3. Click **Network and Internet**.
4. Click **Network and Sharing Center**.
5. Click **View status**.
6. Click **Properties**.
7. Select Internet **Protocol Version 4 (TCP/IP 4)** or **Internet Protocol Version 6 (TCP/IP 6)**
8. Click **Properties**.
9. Click **Advanced**.
10. Select the **WINS** tab.
11. Specify the WINS server IP addresses in the correct search order.
12. Click **OK**.

Configuring iSeries NetServer with the address of the network WINS server:

Using iSeries Navigator, you can configure iSeries NetServer with the address of the network Windows Internet Naming Service (WINS) server.

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 system.

2. Expand **Network** → **Servers**.
3. Click **TCP/IP**.
4. Right-click **iSeries NetServer** and select **Properties**.
5. Select the **WINS Configuration** tab.
6. Click **Next start**.
7. 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 you start iSeries NetServer.
8. 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 you start iSeries NetServer.
9. 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 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.
10. Specify whether you want to enable or disable the iSeries NetServer to act as a WINS proxy.
11. Click **OK** to save your changes.

PC client LMHOSTS static configuration files

In large distributed networks, LMHOSTS static configuration files are helpful for mapping system names to IP addresses.

Connecting your PC client with LMHOSTS

The operating systems on the supported PC client can provide static configuration files that map 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. However, static configuration files are useful 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 system names to IP addresses. The `LMHOSTS` file contains IP addresses and system names. You can use these files to map the IP address for both the system and iSeries NetServer. Mapping the IP address for both the system and iSeries NetServer allows clients to find the system and iSeries NetServer in a large distributed network environment.

You can also add an entry into the `LMHOSTS` file that points to an `LMHOSTS` file that is administered centrally on the i5/OS operating system. By pointing all clients to the central file on the system, 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
10.5.10.1 QNETSERVER #PRE
```

For example, if the iSeries NetServer is a logon server, you can add the following entry to the LMHOSTS file:

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

Related concepts

"iSeries NetServer User Datagram Protocol broadcasts" on page 7
A system that is placed in the same workgroup (domain) and the same subnet (network segment) as the PC client uses iSeries NetServer User Datagram Protocol (UDP) broadcasts.

Finding iSeries NetServer on the network

Finding iSeries NetServer on the network by using your PC client allows you to access shared resources on the network. This also ensures that your connection method to iSeries NetServer is running.

Finding 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 iSeries NetServer name.

For Windows Server 2003:

1. Open **Windows Explorer**.
2. Expand **My Network Places** → **Entire Network** → **Microsoft Windows Network**.
3. Expand the domain or workgroup in which iSeries NetServer is located.
4. Select the iSeries NetServer name.

For Windows Vista:

1. Click the **Start** button to open the **Start** menu.
2. Select **Network**.
3. Select the iSeries NetServer server name.

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 iSeries NetServer name.

For Windows XP or Windows Server 2003:

1. Open **Windows Explorer**.
2. Expand **My Network Places → Entire Network → Microsoft Windows Network**.
3. Expand the domain or workgroup in which iSeries NetServer is located.
4. Select the iSeries NetServer name.

For Windows Vista:

1. Click the **Start** button to open the **Start** menu.
2. Specify the iSeries NetServer server name in the **Start Search** field.
3. Press Enter.

Finding iSeries NetServer from Windows Search

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 iSeries NetServer server name.
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 iSeries NetServer server name 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 iSeries NetServer server name in the appropriate field.
7. Click **Search**.

Windows clients support the addressing of systems by using both fully qualified names and 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 NetServer with a Windows client. For example, you can 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 Windows command prompt, as in the following examples:

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

Related tasks

"Accessing file shares from a Windows client" on page 28
You can use your Windows client to access the file shares by using iSeries NetServer.

"Troubleshooting iSeries NetServer location on the network" on page 52
You can use the troubleshooting techniques if you have trouble finding iSeries NetServer on the network.

Related information

iSeries NetServer Linux Client (Samba) Support

Administering iSeries NetServer

Administering iSeries NetServer allows you to manage file and print shares and control other iSeries NetServer functions.

iSeries Navigator is a component of iSeries Access for Windows. It provides the administration interface for iSeries NetServer. By default, iSeries NetServer shares the iSeries Access for Windows installation directory on the network.

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

After installing iSeries Access for Windows and iSeries Navigator, you are ready to administer iSeries NetServer.

Viewing and configuring iSeries NetServer properties

You can view and configure iSeries NetServer properties, such as general settings, security settings, and WINS configuration by using iSeries Navigator.

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** → **Servers**.
3. Click **TCP/IP** to display a list of TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Properties**.

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

Enabling iSeries NetServer support for Kerberos V5 authentication

Kerberos provides strong authentication for client and server applications by using secret-key cryptography. iSeries NetServer also supports Kerberos Version 5 (V5) for user authentication.

To enable iSeries NetServer support for Kerberos V5 authentication, you must first have the iSeries Navigator Security option, Network authentication service, and Enterprise Identity Mapping (EIM) configured on the i5/OS operating system.

You can enable iSeries NetServer support for Kerberos V5 authentication through iSeries NetServer properties. The configuration wizard helps you configure the necessary services required for use with Kerberos V5. You must also complete the additional configuration requirements for Kerberos V5 authentication enablement.

To enable iSeries NetServer support for Kerberos V5 authentication through iSeries NetServer properties, follow these steps:

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 after this support is enabled. The following Windows clients do not support Kerberos V5:
     – Windows 95
     – Windows 98
     – Windows NT
     – Windows Me
5. Click **OK**.

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

Related concepts

"Troubleshooting the logon server" on page 37
You can use these methods to resolve problems with iSeries NetServer and the logon server.

Related information

Network authentication service

Enterprise Identity Mapping (EIM)

Installing iSeries Navigator Security option

You need to install the iSeries Navigator Security option on the i5/OS operating system before enabling iSeries NetServer support for Kerberos V5 authentication.

To install the Security option, follow these steps:

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

Starting iSeries NetServer Configuration wizard

To use Kerberos V5 with iSeries NetServer, additional configuration is required. The configuration wizard helps 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

To use Kerberos V5 authentication with iSeries NetServer, you need to configure Enterprise Identity Mapping (EIM) and Network authentication.

Complete all of the following steps before restarting the system:

1. If you currently have EIM and Network authentication service configured, skip this step and proceed to step 2.

   Note: The EIM configuration wizard gives you the option to configure Network authentication service, if it is not currently configured on your system. In this event, you must select to configure the Network authentication service, because it is a required service to use Kerberos V5 authentication with iSeries NetServer.

   To configure EIM and Network authentication service, complete the following steps:

   a. Open iSeries Navigator and connect to the system with which you want to work.
   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 service is not currently configured on the system, 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 service.

2. If Network authentication service is already configured on your system, 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 can 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 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 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 on page 17 and 3c on page 17 if you want to access iSeries NetServer using additional principal names.

e. Restart the system.

Related information

Network authentication service

Enterprise Identity Mapping (EIM)

Changing the iSeries NetServer server name

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 the i5/OS operating system. Even though you can connect to iSeries NetServer using any name you choose, you should not change the server name from its default. The name should be the same as your system name. However, if you must change the iSeries NetServer server name, review the naming guidelines beforehand. You can view the system name in the i5/OS 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 system name does not take effect until the next time iSeries NetServer is started.

To change the iSeries NetServer system 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** → **Servers**.
3. Click **TCP/IP** to retrieve a list of the TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Properties**.
5. 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 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 conditions 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.

Note: 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 in 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 you configure new Windows clients while the existing clients continue to use (map to) the previous name.

Disabled user profiles

iSeries NetServer uses i5/OS user profiles and passwords to allow network administrators to control how users can access data. In addition, the QMAXSIGN system value specifies how many unauthorized sign-on attempts disable the user profile for iSeries NetServer use.

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 a system with iSeries NetServer. If a user exceeds the maximum number of sign-on attempts, the user profile becomes disabled for iSeries NetServer use only. Other types of access, such as a system sign-on, are not prevented.

iSeries NetServer uses the last-changed date in i5/OS user profiles to determine whether they have changed since becoming disabled. If the last-changed date is newer than the date of becoming disabled, the user profile becomes enabled again for use with iSeries NetServer.

Notes:

1. The QSYSOPR message queue displays the CPIB682 error message, which indicates when an i5/OS 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 i5/OS user profile password, the client can try to access iSeries NetServer several times before displaying the Network Password window. When the correct password is supplied, the user profile might already be disabled for iSeries NetServer use on the system. If you encounter this situation, the maximum sign-on attempts allowed system value, QMAXSIGN, can be increased to accommodate multiple client authentication attempts. You can use the Work with System Values command `WRKSYSVAL SYSVAL (QMAXSIGN)` to change the maximum sign-on times.

Displaying disabled user profiles

You can use iSeries Navigator to display the detailed information about the disabled user profiles.

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

1. From iSeries Navigator, expand ***system*** → **Network** → **Servers**.
2. Click **TCP/IP** to view list of TCP/IP servers available.
3. Right-click **iSeries NetServer** and select **Open**.
4. Click **File** in the upper left corner.
5. On the pull-down menu, select **Disabled User IDs**.

Enabling a disabled user profile

You can re-enable a user profile that has become disabled by using iSeries Navigator or by changing the user profile. You can also enable a disabled user profile by stopping and restarting iSeries NetServer.

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

To use iSeries Navigator to enable a disabled iSeries NetServer user, follow these steps:

Note: You need *IOSYSCFG and *SECADM authority to enable a disabled user profile through iSeries Navigator.

1. From iSeries Navigator, expand ***system*** → **Network** → **Server**.
2. Click **TCP/IP** to view the list of TCP/IP servers available.
3. Right-click **iSeries NetServer** and select **Open**.
4. Click **File** in upper left corner.
5. On the pull-down menu, select **Disabled User IDs**.
6. Click a disabled user ID and select **Enable User ID**.

You can also enable a disabled iSeries NetServer user by changing the user profile. To change the user profile, enter the following command:

```
CHGUSRPRF USRPRF(USERNAME)
```

where *USERNAME* is the name of the user profile you want to re-enable.

You can exit the Change User Profile display without making any changes to the properties for the user profile.

A third way to enable a disabled iSeries NetServer user is to stop and then restart iSeries NetServer.

Related reference

"iSeries NetServer security: Guest versus nonguest" on page 47
Typically you can access iSeries NetServer by using an i5/OS user profile. The guest profile will be used when the requested ID (as sent by Windows or Samba) is not found.

Starting and stopping iSeries NetServer

Starting iSeries NetServer allows you to immediately begin sharing data and printers with your PC clients, while stopping iSeries NetServer ends all sharing of resources. Stopping and then restarting iSeries NetServer also allows you to change iSeries NetServer configuration.

iSeries NetServer starts automatically when TCP/IP is started. If you need to restart iSeries NetServer, follow these steps:

1. Open a connection to iSeries Navigator on your system.
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
```

To stop iSeries NetServer, 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 retrieve a list of TCP/IP servers available.

4. 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
```

Related tasks

"Configuring i5/OS for NetServer" on page 5
To verify whether iSeries NetServer is properly configured, you can use a series of commands.

Administering subsystems for iSeries NetServer

You can administer the subsystems in which user jobs are run. For example, you can create separate subsystems for users or groups of iSeries NetServer users, add prestart jobs to subsystem descriptions, and specify the subsystems.

The QSERVER subsystem is still included with the same default prestart job entries. If a client attempts to use a subsystem that does not have prestart job entries defined, the system then runs in the QSERVER subsystem using batch-immediate jobs. If this occurs, the jobs maintain the same name, but might 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 End TCP/IP Server (ENDTCPSVR) command and the End Server (QZLSENDS) API also take a longer time 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 connection time might also be slightly longer when batch-immediate jobs are used.

Adding prestart jobs to a subsystem description

When you configure clients to run jobs in a different subsystem other than QSERVER, you must also add the necessary prestart jobs to the subsystem description. For example, to add prestart jobs for QZLSFILE in another subsystem, 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 prestart 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 prestart jobs drops below 1, five more prestart jobs are started in order to be used by future connections. For QZLSFILET, there is only one job running in a subsystem.

Specifying subsystems

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

1. From 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.

Related concepts

"Troubleshooting user profile connections" on page 48
When you try to access a file share, errors might occur because of user profile problems.

Setting 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 i5/OS user profile. According to the needs, you can grant different levels of authority to different guests by setting the guest user profile.

You can set the user profile that iSeries NetServer uses for guest users using iSeries Navigator. You can also specify what level of authority guests will have to i5/OS shared resources using iSeries NetServer. You need input/output system configuration (*IOSYSCFG) and security administrator (*SECADM) special authority to change the guest user profile information. The change to the guest user profile does not take place until the next time 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** → **Servers**.
3. Click **TCP/IP** to retrieve a list of TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Properties**.
5. Go to the Advanced dialog box and click **Next Start**.
6. In the **Guest User Profile** field, enter the user profile that you want guests to have when they use iSeries NetServer.

   Notes:

   a. If you leave this field blank, then unknown users do not have access to resources through iSeries NetServer.
   b. The guest user profile that you specify cannot have any special authorities. Guests should have little or no authority on the i5/OS operating system.

Related concepts

"Guest user profiles" on page 40
iSeries NetServer supports guest user profiles, also known as an *anonymous user profile*.

Viewing iSeries NetServer status

The iSeries NetServer Status dialog box contains important statistical information that can help you to effectively administer iSeries NetServer.

You can refresh the current statistics for the system, 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 that you do not have to refresh each time the iSeries NetServer Status dialog box is opened. Timed refresh values are saved for each system, not for each user.

To display iSeries NetServer status, 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 **Status**.

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

Viewing a list of iSeries NetServer shared objects

You can view a list of the objects that iSeries NetServer is currently sharing by using iSeries Navigator or Windows clients.

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

- **File shares**, which share integrated file system directories on the i5/OS operating system
- **Print shares**, which share i5/OS output queues

Viewing a list of iSeries NetServer shared objects using iSeries Navigator

Using iSeries Navigator, you can view a list of objects that the i5/OS operating system is currently sharing with PC clients by using iSeries NetServer.

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

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

Viewing a list of iSeries NetServer shared objects using Windows clients

Using Windows clients, you can view a list of objects that the i5/OS operating system is currently sharing with PC clients by using iSeries NetServer.

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 iSeries NetServer server name.
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. In the **Computer Name** field, specify the iSeries NetServer server name.
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. In the **Computer Name** field, specify the iSeries NetServer server name.
7. Click **Search**.
8. Open iSeries NetServer by double-clicking the found computer.

For Windows Vista:

1. Open the Windows **Start** menu.
2. In the **Start Search** field, specify the iSeries NetServer server name.
3. Press Enter.
4. 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 i5/OS 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.

Viewing and configuring 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** → **Servers**.
3. Click **TCP/IP** to retrieve a list of the TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Open**.
5. Expand **Shared Objects**.
6. 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.

Viewing shared object status

Viewing the current statistics for a shared object connection to iSeries NetServer through iSeries Navigator, you can acquire information such as workstation name, user name, share type, and time connected.

You cannot change or reconfigure shared object statistics because they are records that contain information only.

To display iSeries NetServer shared object status, 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 **Open**.
5. Expand **Shared Objects**.
6. Select a shared object.
7. Right-click the session connection and select **Status**.

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

Viewing 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. You can view a list of active iSeries NetServer sessions.

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

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

Viewing 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 i5/OS 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** → **Servers**.
3. Click **TCP/IP** to retrieve a list of the TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Open**.
5. Expand **Sessions**.
6. 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 there are open files for that session.
2. Multiple users can be active from the same workstation. 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 can decide to end them all and optionally establish new sessions.

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

Viewing 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, 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 a TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Open**.
5. Expand **Sessions**.
6. Select a session.
7. Right-click the session connection and select **Status**.

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

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

Stopping an iSeries NetServer session

iSeries NetServer supports multiple users, including guests, logged on from the same workstation. You can end single or multiple user sessions on a workstation to stop a client's use of file and print shares on a specific session.

If multiple users are active from the same workstation, ending a user session ends only the iSeries NetServer file and print activity for that session. In addition, ending an active iSeries NetServer session stops the client's 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** → **Servers**.
3. Click **TCP/IP** to retrieve a list of TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Open**.
5. Expand **Sessions**.
6. 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 system and using iSeries NetServer again.

File shares

An iSeries NetServer file share is a directory path that iSeries NetServer shares with clients on the network.

A file share can consist of any integrated file system directory on the i5/OS operating system. You can create, display, configure, and end iSeries NetServer file shares.

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

Related concepts

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

Creating an iSeries NetServer file share

You can share any directory in the i5/OS integrated file system with clients in the network by using iSeries NetServer. Creating a file share allows PC clients to easily access resources on the system.

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** → **Servers**.
3. Click **TCP/IP** to retrieve a list of TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Open**.
5. Right-click **Shared Objects** and select **New** and then **File**.
6. Use the General Properties page to configure the new file share with a name, description, access, maximum number of users, and directory path name.
7. Use the Text Conversion page to identify which file types must have their contents converted from the i5/OS file coded character set ID (CCSID) to the CCSID you specify for the share.

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

Controlling access to iSeries NetServer file shares

You can assign an access setting for iSeries NetServer file shares to control the PC clients' level of access to objects in the directory paths of the i5/OS integrated file system.

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

Stopping file sharing

You can stop file sharing with the other clients.

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

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

Accessing file shares from a Windows client

You can use your Windows client to access the file shares by using iSeries NetServer.

To access file shares by using a Windows client, you can either map file shares to logical drives or use Universal Naming Convention (UNC) mapping. However, working with logical drive letters might be easier.

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 can enter the following syntax:
   ```
   \\QSYSTEM1\Sharename
   ```
   Note: `QSYSTEM1` is the iSeries NetServer server name on the i5/OS operating system, and `Sharename` is the name of the file share you want to use.
5. Click **OK**.

Related tasks

"Finding iSeries NetServer on the network" on page 13

Print shares

A *print share* is an output queue that is shared with PC clients on the network. You can share any i5/OS output queue with the clients by using iSeries NetServer.

You can create, display, configure, and end print shares. A print share consists of any i5/OS 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 system. If autoselect is not used, the spooled file type must correspond exactly to the output queue destination, or you will receive a print error.

Creating a print share

You can share any i5/OS output queue with PC clients in the network by creating an iSeries NetServer print share.

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** → **Servers**.
3. Click TCP/IP to retrieve a list of the TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Open**.
5. Right-click **Shared Objects** and select **New** and then select **Printer**.

6. In the **General - Properties** dialog box, configure the new print share with a name, description, output queue, library, printer driver, spooled file type, and printer file.

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

PC client print device drivers for use with print shares

iSeries NetServer acts as a print server that makes the services of the i5/OS network print server available to PC clients. The network print server provides client access to i5/OS print objects and resources.

Network Print Server allows clients with the correct print device drivers to spool print jobs onto i5/OS output queues of various spooled file types. These spooled file types are as follows:

- 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 the following ways:

- AFP print device drivers are available for free download from the IBM Printing systems Web site (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 can find the AFP and SCS print device drivers.

Stopping print sharing

You can stop print sharing by using iSeries Navigator.

To stop print sharing from iSeries Navigator, 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 retrieve a list of the TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Open**.
5. Expand **Shared Objects**.
6. Right-click a shared printer and select **Stop Sharing**.

Using print shares with Windows 2000, Windows XP, Windows Server 2003, and Windows Vista client

You can use your Windows client to access i5/OS print shares by using iSeries NetServer.

To use your Windows client to access i5/OS print shares, follow these steps:

For Windows 2000 or Windows XP:

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

For Windows Vista:

1. Click the **Start** button to open the **Start menu**.
2. Select **Network**.
3. Select the iSeries NetServer server name.
4. Open iSeries NetServer by double-clicking the found computer.
5. Right-click a shared printer and select **Open**.
6. In the prompted window, click **Yes** to set up the printer on your computer.
7. In the prompted window, 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**.

Domain logon support

To remove the need for a Windows server to handle domain logon services in a Windows NT domain, iSeries NetServer provides this support.

Windows clients are able to sign on to an iSeries NetServer domain just as they would sign on to an NT domain. iSeries NetServer provides the following services as additional advantages:

- The i5/OS operating system 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 the system, including Desktop, Start Menu, Favorites, and so on.
- Storage, retrieval, and maintenance of Windows system policies from the system.

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 (BDC); nor can it dynamically replicate logon related information to WinNT Domain Controllers.

iSeries NetServer and client PC configuration

You need to install the IBM Network Primary Logon Client (IPLC) product to use the logon server support of iSeries NetServer.

Configure iSeries NetServer 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 use the logon server support. You can download this product 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 IPLC on Windows workstation installations. Never install it on a PC configured as a system or a terminal system because it will conflict with that type of installation and will not allow any user to log on. A PC system does not sign on to another system. Also, remember that iSeries NetServer Domain Logon Support can remove the need for such systems.

Logon server setup

When iSeries NetServer starts as a logon server, you need to take these actions in addition to normal startup.

You need to take the following actions to accomplish the setup:

- You need to check the existence of the NETLOGON share. If this share does not exist, then you should create a directory (/QIBM/UserData/OS400/NetServer/NetLogon) and share the directory as NETLOGON with read-only access. Logon scripts, system policies, and default user profiles can be placed in this directory.
- You should register iSeries NetServer and make sure it listens 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 lists 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 about this error message.

Logon server home directories

The logon server that authenticates the user determines the location of the user's home directory.

Configuring home directories on the logon server

You can configure users to have a home directory that can be collectively backed up and maintained on the system. By default, an i5/OS logon server considers the home directory path stored in the user profile (on the i5/OS operating system) to be the PC client user's home directory. For example, if user JOE has a home directory configured in his user profile as /home/joe, then this path is treated as a Universal Naming Convention (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 so that a Windows 98 client can map a drive to the directory.

Mapping a drive to your home directory

Windows 2000 and Windows XP clients using the IBM Network Primary Logon Client for Windows (IPLC) will attempt to map a drive to the user's home directory automatically when they log on.

Home directories on other systems

Sometimes it is desirable to store user home directories on a server other than the logon server. This might 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 system. 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 system DRACO2, then the home directory field for user JOE can be /qntc/draco2/home. Alternatively, individual home directories can be shared from DRACO2, in which case the home directory would be /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, because this is stored in the user's profile. Then other applications running locally on the system would, in theory, be able to access this same home directory.

Note: Because this configuration also changes the home directory for the local user who signs on to the i5/OS operating system through PC5250, for example, the ramifications of this need to be considered if there is a possibility that the user might sign on directly to a system that is configured as a logon server.

Roaming profiles

When iSeries NetServer is configured as a logon server, it supports roaming profiles. Roaming profiles store their personal PC configuration, including desktop icons, start menu, and registry, on a file server in addition to caching these files locally.

In this way, users can sign on from various computers and always get their same desktop and profile settings. This function is also known as *roving users* and as *profile serving*.

In many network environments, roaming profiles are not necessary because users tend to have their own workstation that they always log in from. And the extra time needed to download and save a personal profile when the function is rarely used might not be justified. However, there are PC environments where users need to move from workstation to workstation, or where they have multiple PCs that should be kept synchronized (perhaps a mobile computer in addition to a desktop 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. Users cannot change their profiles if they are mandatory. Thus, mandatory profiles are downloaded from the server at logon, but are not saved back during logoff.

Configuring user profiles from Windows 2000 and Windows XP clients

Windows 2000 and Windows XP clients 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 to use the support.

To configure user profiles as a logged-on administrator, follow these 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 Profiles** section, click **Settings**.
6. Select the user profile and click **Change Type**.

You can also copy an existing Windows user profile to the server to prime the roaming user profile for a user. From the User profile dialog box you opened in the previous procedures, click the **Copy to** button. Locally cached profiles (preferences and settings) can be replicated to the logon server just as 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. If you are migrating multiple profiles from an NT server to an i5/OS logon server, then it will probably be more efficient to copy over the entire \WINNT\Profiles folder.

By default, clients with the IBM Network Primary Logon Client for Windows (IPLC) attempt to load or store roaming profiles in the Profiles subdirectory of the user's home directory. To override this behavior, you can change the configured user profile path by completing the following steps:

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 at \\logonserver\profilesShare\ profileDirectory

Mandatory profiles

Mandatory profiles are roaming profiles that are not updated when the user logs off.

Even if the users change their desktop settings while logged on, the changes are not 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 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 are not set up the exact same way (installed programs, folders, and so on), then the shortcuts might not be valid, and you might see a series of errors for invalid shortcuts when you log on in these situations.

Because most items stored on the desktop or in the Start folder are shortcuts, it is better 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. Because different types of information are stored in each case, you might 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 information is saved independently during logoff for each logon. Therefore, the last client being logged off will reflect the actual changes saved to the profile.

You might receive a message that indicates that your roaming profile is not available. You will be logged on with your local profile. This typically means that the roaming profile might not be found in the expected place.

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

Users store files other than shortcuts on their desktop. If these files are large, it can significantly slow down the logon process. A workaround is to specify certain profile subfolders not to 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 on the logon server. By default, the NETLOGON share is /QIBM/UserData/OS400/NetServer/NetLogon for iSeries NetServer. Special naming conventions must be followed for an i5/OS 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. Assume a user name of KRISTY, who is a member of the i5/OS Primary Group PCGROUP.

1. If the file KRISTY.BAT (case does not matter for file systems that are not case sensitive) 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.

Note: If you do not restart iSeries NetServer after placing a new user or a group logon script in the NETLOGON share, the script might not be picked up by the user at the next logon. This is 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 by using the IBM Network Primary Logon Client (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 i5/OS operating system called ADMINISTRA (10-character maximum), then the first logon script file checked for is ADMINI .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%.

Here 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%\%userna %

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

Policies are a batch of changes applied to the PC's registry that controls and restricts a number of things.

Policies can be used to control and restrict 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.

Policy serving in a System i domain is similar to policy serving in a Windows 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.

When you edit a policy file, you are making changes based on a template that you select. Templates specific to Windows include common.adm, winnt.adm, and windows.adm. Other applications might provide their own templates that allow the restriction of certain functions in the application. iSeries Access provides several templates.

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) systems 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 careful when you put system policies into effect. You can easily lock out a function that you did not intend to on a PC. Because policies are applied to the local registry, it remains locked out until you specifically turn it back on in the policy file. The change can be picked up during the next logon if you turn it back on in the policy file.

Browsing support

Browsers maintain the list of computers for their respective domain and a list of accessible domains.

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). The role of the MB includes being the Domain Master Browser (DMB) for the domain and a Local Master Browser (LMB) for the subnet.

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 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.

Reducing message questions from roaming users logging on from Windows NT, Windows 2000, and Windows XP

You might see a message similar to one of the following messages 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 tasks 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: If the logon server is unavailable, this user is signed on with the default local user profile.

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 easier.

1. Choose an iSeries NetServer name 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, and so on.

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.

Using 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.

Troubleshooting the logon server

You can use these methods to resolve problems with iSeries NetServer and the logon server.

Cannot find the logon server

If your PC cannot contact the logon server, you might see a message similar to one of the following messages:

- `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 might occur for various reasons:

- The client cannot resolve to the logon server. This is the most common reason and there can be a variety of causes, depending on 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:
  - **Microsoft Browsing protocol**

    You can use the domain discovery support of the Microsoft Browsing protocol. The i5/OS browsing support is discussed in "Browsing support" on page 36. The basic idea is that if at least one browser server for the domain exists in the subnet from which the PC will log on and that Local Master Browser (LMB) has knowledge of the Domain Master Browser (DMB), then the client can ask it for the name of the logon server, after which normal name resolution can proceed (DNS, and so on.). 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.
  - **Windows Internet Name Service (WINS)**

    WINS 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.
  - **LMHOSTS configuration file**

    You can also make use of the 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.

    Notes:

    - LMHOSTS files can include files on systems so that this solution can still be centrally administered.
    - 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 might not work. However, a trick that often works for Windows

2000 or Windows XP clients is to change the workgroup of the client system to one that is different from the domain name assigned to iSeries NetServer.

- iSeries NetServer is not started or it does not start as a logon server for the domain in question. Check whether it is properly configured as a logon server and make sure that there are no conflict messages in the QSYSOPR message queue. If you see message CPIB687, read the detailed description for more information about the exact nature of the conflict.

User name cannot be found

This message normally indicates that the user attempting to log on does not have a user profile on the i5/OS logon server. A guest user might not be able to sign on to an i5/OS domain. In extreme cases where the logon server is busy or slow, the logon information might not be cached quickly enough by the iSeries NetServer. If this is the case, you might need to try to log on again.

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 i5/OS user profile. Use your i5/OS password and try again.
- The password in your i5/OS profile has expired. Unfortunately, you cannot change your i5/OS password through Windows, so this must be directly done to your profile.
- Your i5/OS 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 system is being resolved to. Preface the user name with the domain name in the logon prompt like this: *domain\user*, where user is the user name 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, you will see a message indicating that the system cannot log you on. Your network account and password are correct, but your local account password is out of synchronization. Contact your administrator.

Cannot find the iSeries NetServer domain through My Network Places

Assume that 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. Here are some possibilities:

- 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 cannot see my home drive mapped for Windows 2000 or Windows XP clients even though the share name exists

The typical problem 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 i5/OS operating system, 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, enter the CRTDIR '/home/USER1' command.

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

You must be logged onto the target domain with an administrator profile (not the profile you want to change to roaming) in order for the option to be available. iSeries NetServer is able to map longer Windows user names to truncated i5/OS profile names. Thus, you can do the following tasks:

1. Create the user profile ADMINISTRA on the i5/OS operating system.
2. Give ADMINISTRA a password that matches the password for administrator on the client.
3. Log onto the i5/OS domain with the administrator profile.
4. Open Control Panel, and then open System.
5. Click the **User Profiles** tab and make the appropriate changes.

My profile is listed as Roaming, but changes to my settings (or desktop, and so on) 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 might be the problem if you try to log on from a different workstation and you do not 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. Check for the following items:

- Make sure that the appropriate access rights are set on each part of the path on the logon server.
- Make sure that the path is spelled correctly if it is being specified in the user profile settings on the workstation.
- Check that unsupported environment variables are not being used. Some environment variables are not active or usable until the logon succeeds. 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 is unable to resolve the %logonserver% environment variable. Try using \\servername\profiles\username instead.
- Preferably, start with a locally cached profile that is copied to the logon server.

Locally stored profile is newer than that on the server

When you log on, a dialog box is displayed to ask if you want to use your local copy instead. Normally, you can respond with Yes to this invalid message. In this way, you can reduce the network traffic, or you will repeatedly receive this message after logging off from the same workstation. For example, 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 the profile to the logon server. Ensure that the client's time is synchronized 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 i5/OS operating system using a traditional password, when the iSeries NetServer has Kerberos authentication enabled.

Related tasks

"Enabling iSeries NetServer support for Kerberos V5 authentication" on page 15
Kerberos provides strong authentication for client and server applications by using secret-key cryptography. iSeries NetServer also supports Kerberos Version 5 (V5) for user authentication.

iSeries NetServer security

Using iSeries NetServer securely ensures that unauthorized users do not have access to iSeries NetServer resources, configuration, or shared data.

When you take steps to ensure iSeries NetServer security, only authorized users can access iSeries NetServer resources and change iSeries NetServer configuration properties.

User profile authority requirements

You can secure iSeries NetServer by controlling i5/OS user profile authorities.

iSeries NetServer authenticates client files and print requests that are based on the user identity (user ID) and password that are used in the Windows desktop logon. If an i5/OS user profile matches the Windows desktop client user ID, then the passwords are checked. If the passwords do not match, iSeries NetServer prompts 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 i5/OS operating system), then iSeries NetServer truncates the Windows user ID to 10 characters and attempts to match it with an i5/OS user profile. For example, an i5/OS user profile called ADMINISTRA can be created to match the Windows Administrator user without requiring guest support.

In order to access iSeries NetServer shared resources, clients might not need an i5/OS 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.

To configure this support, follow these steps:

1. Right-click 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 authorities 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 i5/OS integrated file system directories and output queues that are used for basic file and print services.

Guest user profiles

iSeries NetServer supports guest user profiles, also known as an *anonymous user profile*.

The i5/OS operating system 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 few authorities because the guest user is considered a nontrusted user.

Related tasks

"Setting the guest user profile for iSeries NetServer" on page 22
A guest user profile provides a base level of access for clients who do not have a valid i5/OS user profile. According to the needs, you can grant different levels of authority to different guests by setting the guest user profile.

Hiding 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** → **Servers**.
3. Click **TCP/IP** to display a list of TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Properties**.
5. Click the **Advanced** tab and click the **Next Start** button.
6. 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 might cause problems for logon services for some networks. In general, the default browsing announcement interval should be kept if iSeries NetServer is a logon server. The default browsing announcement interval is 720 seconds, or 12 minutes.

Related reference

"iSeries NetServer does not appear in Windows My Network Places" on page 45
iSeries NetServer might not appear in Windows My Network Places for a variety of reasons.

Requiring 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** → **Servers**.
3. Click **TCP/IP** to display a list of TCP/IP servers available.
4. Right-click **iSeries NetServer** and select **Properties**.
5. Click the **Security** tab and click the **Next Start** button.
6. From the **Require clients to sign requests** drop down box, choose **Yes**, **Optional**, or **No**.

Using Windows messenger service with iSeries NetServer

iSeries NetServer can automatically send informational messages to users in some situations.

Under the following situations, iSeries NetServer automatically sends informational messages:

- The user password is about to expire.
- The 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.

Related concepts

"Troubleshooting iSeries NetServer using Windows messenger service" on page 53
You can use Windows messenger service to troubleshoot problems with iSeries NetServer.

"What's new for V5R4" on page 1
This topic highlights the changes made to the iSeries NetServer topic collection for V5R4.

Configuring the clients

For client workstations to receive informational messages, the messenger service must be active.

You must configure your PC clients to activate this service.

Configuring clients on Windows 2000 and Windows XP

You can configure clients on Windows 2000 and Windows XP operating system to receive informational messages.

To configure the clients on the Windows 2000 and Windows XP operating system, follow these steps:

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

Configuring clients on Windows Server 2003

You can configure clients on Windows Server 2003 to receive informational messages.

To configure the clients on the Windows 2000 and Windows XP operating system, follow these steps:

1. Click **Start** → **Control Panel**.
2. Open **Services** from **Administrative Tools**.
3. Scroll down to find Messenger.
4. Ensure that the status is **Started** and the **Startup** type is **Automatic**. To start WinPopup.exe, follow these steps:
   a. Click **Start** → **Run**.
   b. Type `winpopup.exe` in the Open field.
   c. Click **OK**.

Configuring clients on Linux

You can configure the clients on the Linux operating system to receive informational messages.

To configure the clients on Linux, follow these steps:

1. Enable Samba's messenger support. Edit the smb.conf file so that it contains a message command directive. Here 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 place the messages into a window in the background. Here 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 want to 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 &.

Enabling iSeries NetServer for messaging specific to Windows

Administrative alerts are turned off by default. You can enable iSeries NetServer for messaging specific to Windows.

To enable messaging specific to Windows, 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 **Properties**.
5. Click the **Advanced** tab and click the **Next Start** button.
6. Click the check box next to **Allow administrative alerts**.
7. Specify the **Minimum message severity**. Valid values are from 0 to 99.

Associated i5/OS messages

Some i5/OS messages have been added to accommodate messaging support specific to Windows.

These messages are not issued on the i5/OS operating system. Only the text of the messages is used (with replacement) to send as a network message to the client user attempting to connect.

These messages are as follows:

CPIB68A
No user profile found for user &1.

CPIB68B
The profile for user &1 is disabled.

CPIB68C
The password for user &1 is expired.

CPIB68D
No password exists for user &1.

CPIB68E
User &1 is disabled for iSeries NetServer access.

CPIB68F
User &1 was enabled for iSeries NetServer access.

CPIB690
Password for user &1 will expire in &2 day(s).

CPIB691
User &1 has successfully connected.

CPIB692
User &1 encountered Kerberos error &2 connecting through iSeries NetServer.

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

Displaying a log of the message send attempts

To display a log of network messages that the server attempted to send, you can use the iSeries NetServer maintenance program.

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 spooled file in the QSECOFR output queue. Use the Work with Spooled Files (WRKSPLF QSECOFR) command to display the queue.

Example: Spooled 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.

Sending custom messages through iSeries NetServer

If you have built the GO NETS tools for iSeries NetServer using the QUSRTOOL library support, you can use the Send NetServer Message (SNDNSVMSG) command to send custom messages to registered users on the network.

The Send NetServer Message (SNDNSVMSG) 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.

Examples

Sending a Windows message to user name JOE1 on the network and to user KRISTY on client machine WORKSTATION1

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

Because 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
```

Sending a Windows message to all users who have 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.

Sending a 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.

Tips and techniques

These tips and techniques help solve problems or make iSeries NetServer work more efficiently for you.

iSeries NetServer does not appear in Windows My Network Places

iSeries NetServer might not appear in Windows My Network Places for a variety of reasons.

iSeries NetServer takes advantage of the Microsoft proprietary browsing protocol, which allows iSeries NetServer 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, because iSeries NetServer does not support NetBIOS, when you transfer these lists, you might lose those 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 might not be complete if some servers are 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 might also be hidden from the network because of the interval setting for browse announcement.

Related tasks

"Hiding iSeries NetServer from the network" on page 41
For an added measure of security, you can hide iSeries NetServer from the Windows My Network Places.

iSeries NetServer fails to start

If iSeries NetServer fails to start, you can view the message in the QSYSOPR message queue. Use this message to find the cause of the problem.

The message reads as follows:

```
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 about this message to help you find the cause of the problem.

Starting iSeries NetServer at initial program load

iSeries NetServer can be started and ended as an individual TCP/IP server by using the Start TCP/IP Server and End TCP/IP server commands.

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 called. 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 follow the following steps to find this dialog box:

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

The 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 nonguest

Typically you can access iSeries NetServer by using an i5/OS user profile. The guest profile will be used when the requested ID (as sent by Windows or Samba) is not found.

The guest user profile allows the file and print sharing by users who otherwise would not require an i5/OS user profile.

When using iSeries NetServer, normal i5/OS user profiles and passwords apply. By default, only users with valid i5/OS user profiles and passwords can access resources on the system. Windows 2000, Windows XP, and Windows Server 2003 offer the option to select a different user ID. If the passwords do not match, you will see a password window. Windows can optionally be set to remember the password.

An i5/OS 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 i5/OS system value name, QMAXSIGN, specifies how many unpermitted access attempts disable a user profile. The Windows operating system will try to access again when denied. So it might 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.

If a user profile is not found that matches the user ID that is used to access iSeries NetServer, you can use an optionally configurable guest user profile. This guest, created by the i5/OS 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 file and print sharing by users who otherwise would not require an i5/OS 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.

Related tasks

"Enabling a disabled user profile" on page 20
You can re-enable a user profile that has become disabled by using iSeries Navigator or by changing the user profile. You can also enable a disabled user profile by stopping and restarting iSeries NetServer.

API guides

You can access all of the administrative functions that are available through iSeries Navigator by using i5/OS application programming interfaces (APIs). This means that you can administer iSeries NetServer through your CL, COBOL, RPG, C, and C++ programs.

The following list shows 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)

Related information

Application programming interfaces

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 you save the entire i5/OS operating 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.

This is the location of the iSeries NetServer configuration and share data files on the system: /QIBM/UserData/OS400/NetServer.

The following specific files are needed:

- **Qazlscfg**: The file contains configuration information.
- **Qazlsshr**: The file contains share information.
- **Qazlsext*xxx***: The file 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 about these commands and other useful save and restore options, see Backup and Recovery  (about 8028KB).

Troubleshooting iSeries NetServer

The problems you encounter when you use iSeries NetServer might relate to the status of iSeries NetServer, the PC client connections, or the user profile.

You might experience various difficulties when trying to locate iSeries NetServer on the System i network or using iSeries NetServer resources. Troubleshooting iSeries NetServer helps to solve the specific problems.

Troubleshooting user profile connections

When you try to access a file share, errors might occur because of user profile problems.

- **Lack of authorization**

  User profiles might 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 might be unable to use iSeries NetServer if they attempt to connect to the i5/OS operating system with an incorrect password too many times. If this occurs, then the system 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 the i5/OS operating system or iSeries Access for Windows, but it does stop the user profile from accessing iSeries NetServer.

Note: Management Central has a function to monitor messages from the QSYSOPR message queue. An administrator can use this function to be alerted to profiles being disabled for iSeries NetServer use. The administrator can 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 or client the QZLSFILE job is servicing. A QZLSFILET job might have numerous messages in the job log because it services multiple 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 names, logon types, and server sessions 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.

  As of V5R4, iSeries NetServer by default services file shares in a multithreaded 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. 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. Because 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 avoid starting the QZLSFILET job in the QSERVER subsystem (or other user subsystems). This might involve configuring user subsystems in iSeries Navigator so that some clients run threaded and others run nonthreaded. 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 needs to be specified instead of QSERVER along with its correct library (the program remains the same).

  Programs created with the activation group new ACTGRP(*NEW) option will cause multithreaded jobs to end when the program returns. Therefore, when clients might run in a threaded environment (QZLSFILET job), a program created with ACTGRP(*NEW) should not be registered for exit point QIBM_QPWFS_FILE_SERV.

- **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.

Related tasks

"Troubleshooting file share problems" on page 51
If you experience problems with iSeries NetServer file share readiness, check the status of iSeries NetServer on the system.

"Administering subsystems for iSeries NetServer" on page 21
You can administer the subsystems in which user jobs are run. For example, you can create separate subsystems for users or groups of iSeries NetServer users, add prestart jobs to subsystem descriptions, and specify the subsystems.

Related information

Activation groups and threads

Troubleshooting file share directory paths

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

If you have specified a directory path for a file share, but the directory path does not exist on your i5/OS operating system, then clients will receive an error. The directory path that you specify on the File Share General-Properties dialog box must exist on the system for clients to avoid an error.

Troubleshooting print share problems

You might experience problems when using an iSeries NetServer network printer online for a variety of reasons.

- The network printer might not work online because the user does not have authorization to the i5/OS 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 might experience difficulty with spooling print jobs to an i5/OS output queue when using an iSeries NetServer print share. For iSeries NetServer print shares to function properly, the network print server must be running. If you do not start Network Printing Server, 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.

Troubleshooting print problems when using guest support

When you use the iSeries NetServer guest support to access the i5/OS output queues, you might experience trouble when trying to access the server. In addition, your specified printer might not go online.

If this is the case, you must add a password to the iSeries NetServer guest user profile, for example, SMBGUEST. You must also ensure that you enable the user profile. The network print server 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.

Troubleshooting PC client connection problems

You can test whether your connection method to iSeries NetServer (for example, Domain Name System) is running if you experience connection problems.

To test your connection, follow these steps:

1. Open a Windows command prompt from your PC client.
2. Enter the PING command to test your client connection to the i5/OS operating system. For example, you can ping iSeries NetServer by entering this command:

   ```
   ping QSYSTEM1
   ```

   Note: QSYSTEM1 is the server name of iSeries NetServer on the i5/OS operating system.

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 to the system is working.

Tips:

- Run nbtstat -A *ip-address-of-server* from a command prompt on the client to check connectivity: `C:\WINDOWS>nbtstat -a qnetserver`. If the name of the system is unknown or cannot be resolved, the use of nbstat can also be helpful.
- Another way to check client connectivity to the system is to see whether 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 names, logon types, and system sessions is displayed.

Troubleshooting file share problems

If you experience problems with iSeries NetServer file share readiness, check the status of iSeries NetServer on the system.

To check the status of iSeries NetServer, follow these steps:

1. Verify that the system has started the QSERVER subsystem. If the system has not already started the QSERVER subsystem, then start it by using the Start Subsystem (STRSBS) CL command.
2. Verify that the system has started the QZLSSERVER job within QSERVER. If the system 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 required, verify that the QZLSFILET job is awaiting client requests for file or print serving (TIMW or TIMA status on the Work with Active Jobs display).

   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 threadsafe file shares. There are multiple QZLSFILE jobs in a subsystem, and each one supports one client and all of the thread unsafe 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.

   Related concepts

   "Troubleshooting user profile connections" on page 48
   When you try to access a file share, errors might occur because of user profile problems.

Troubleshooting print device driver problems

You might notice unreadable printed text when using the Advanced Function Printing (AFP) print device drivers that you download from the IBM Printing systems 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:

- Turn off **Font Substitution** and turn on **Create Inline Form Definition** in the printer properties on your PC.
- Install license program AFP Fonts 5769FN1 and AFP DBCS Fonts 5769FNT on your i5/OS operating system.

  For more information about installing license programs, see the Software Installation book  .

Troubleshooting iSeries NetServer using the QSYSOPR message queue

The system operator's message queue, QSYSOPR, contains important information for troubleshooting iSeries NetServer. Messages are logged to the QSYSOPR message queue each time 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 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 system name. You might 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.
```

Troubleshooting iSeries NetServer location on the network

You can use the troubleshooting techniques if you have trouble finding iSeries NetServer 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 system name.
3. Verify that you have configured your PC client to properly resolve the iSeries NetServer system name to an Internet Protocol (IP) address. Configure your PC client to resolve the iSeries NetServer system name to an IP address in one of the following ways:
   - Map the iSeries NetServer system name to its IP address by using the Domain Name System (DNS).
   - Map the iSeries NetServer system name to its IP address by using the Windows Internet Naming Service (WINS).
   - Map the iSeries NetServer system name to its IP address by adding an entry to the LMHOSTS file.

Related tasks

"Finding iSeries NetServer on the network" on page 13

Troubleshooting iSeries NetServer using Windows messenger service

You can use Windows messenger service to troubleshoot problems with iSeries NetServer.

A user trying to connect to a share through iSeries NetServer might be denied access for the following reasons:

- The password does not match.
- There is 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. Support has been added to iSeries NetServer to allow 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.

Related concepts

"Using Windows messenger service with iSeries NetServer" on page 41
iSeries NetServer can automatically send informational messages to users in some situations.

Code license and disclaimer information

IBM grants you a nonexclusive copyright license to use all programming code examples from which you can generate similar function tailored to your own specific needs.

| SUBJECT TO ANY STATUTORY WARRANTIES WHICH CANNOT BE EXCLUDED, IBM, ITS
| PROGRAM DEVELOPERS AND SUPPLIERS MAKE NO WARRANTIES OR CONDITIONS EITHER
| EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR
| CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND
| NON-INFRINGEMENT, REGARDING THE PROGRAM OR TECHNICAL SUPPORT, IF ANY.

| UNDER NO CIRCUMSTANCES IS IBM, ITS PROGRAM DEVELOPERS OR SUPPLIERS LIABLE FOR
| ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY:

| 1. LOSS OF, OR DAMAGE TO, DATA;
| 2. DIRECT, SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC
| CONSEQUENTIAL DAMAGES; OR
| 3. LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS.

| SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF DIRECT,
| INCIDENTAL, OR CONSEQUENTIAL DAMAGES, SO SOME OR ALL OF THE ABOVE LIMITATIONS
| OR EXCLUSIONS MAY NOT APPLY TO YOU.

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.

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.

Programming Interface Information

This iSeries NetServer documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

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
| i5/OS
| IBM
| IBM (logo)
| iSeries
| Netfinity
| NetServer
| OS/400
| Redbooks
| System i

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

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. 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