SYBASE®

Configuration Guide

Sybase® Adaptive Server® Enterprise

Version 12.0

Windows 95, Windows 98, and Windows NT

Document ID: 38421-01-1200-01

Last revised: October 1999

Sybase, Inc., 6475 Christie Avenue, Emeryville, CA 94608.

Contents

About This Book

This manual, *Configuration Guide for Windows 95, Windows 98 and Windows NT*, covers the following topics:

- Configuring Sybase® Adaptive Server® Enterprise, Backup Server™, Adaptive Server Enterprise Monitor™ Server, and XP Server™
- Creating network connections
- Configuring optional functionality, such as Sybmail
- Performing operating system administration tasks
- Working with system administration issues that are relevant to Adaptive Server running on Windows 95, Windows 98 and Windows NT. This manual supplements the *System Administration Guide* and the *Performance and Tuning Guide.*

Audience

This manual is for System Administrators or other qualified installers who are familiar with their system's environment, networks, disk resources, and media devices.

How to Use This Book

This manual contains the following chapters:

Table 1: Windows NT configuration chapters and descriptions

See	To
Chapter 1, "Overview of Adaptive Server Enterprise"	Become familiar with Adaptive Server and its functionality.
Chapter 2, "Beginning Adaptive Server Configuration"	Change the default server names and their basic features after installing Adaptive Server Enterprise version 12.0
Chapter 3, "Setting Up Communications Across the Network"	Configure Adaptive Server to communicate with clients and other servers over the network.
Chapter 4, "Tuning Your Operating System to Adaptive Server"	Set up your operating system to work with Adaptive Server.
Chapter 5, "Logging Error Messages and Events"	Configure the logging of error messages and event messages sent from Adaptive Server.

See	To
Chapter 6, “Using Security Services with NT LAN Manager”	Take advantage of NT LAN Manager for added security on Adaptive Server.
Chapter 7, “Using E-mail with Adaptive Server”	Configure Sybmail to direct Adaptive Server to distribute messages automatically.
Chapter 8, “Managing Adaptive Server Databases”	Learn the basics of database administration with Adaptive Server.
Chapter 9, “Troubleshooting Network Connections”	Learn the basics for troubleshooting network connections with Adaptive Server .
Appendix A, “Adaptive Server Registry Keys”	Learn about the NT Registry keys and values that Adaptive Server uses.

Related documents

The following documents comprise the Sybase Adaptive Server Enterprise documentation:

- The release bulletin for your platform – contains last-minute information that was too late to be included in the books.

  A more recent version of this release bulletin may be available on the World Wide Web. To check for critical product or document information added after the release of the product CD, use the Sybase Technical Library Product Manuals web site.

  To access release bulletins at the Technical Library Product Manuals web site:

  a Go to Product Manuals at http://sybooks.sybase.com.

  b Select a product family link.

  c Select a product link.

  d From the Collection list in the left frame, select the “platform-specific” link for the product and version you are interested in.

  e From the list of individual documents in the right frame, select the link to the release bulletin for your platform.

  Browse the document online or download a PDF version by clicking the PDF button at the bottom of the left frame.

- The Adaptive Server installation guide for your platform – describes installation, upgrade, and configuration procedures for all Adaptive Server and related Sybase products.

- *What's New in Adaptive Server Enterprise?* – describes the new features in Adaptive Server version 12, the system changes added to support those features, and the changes that may affect your existing applications.
- *Transact-SQL User's Guide* – documents Transact-SQL, Sybase's enhanced version of the relational database language. This manual serves as a textbook for beginning users of the database management system. This manual also contains descriptions of the *pubs2* and *pubs3* sample databases.
- *System Administration Guide* – provides in-depth information about administering servers and databases. This manual includes instructions and guidelines for managing physical resources, security, user and system databases, and specifying character conversion, international language, and sort order settings.
- *Adaptive Server Reference Manual* – contains detailed information about all Transact-SQL commands, functions, procedures, and datatypes. This manual also contains a list of the Transact-SQL reserved words and definitions of system tables.
- *Performance and Tuning Guide* – explains how to tune Adaptive Server for maximum performance. This manual includes information about database design issues that affect performance, query optimization, how to tune Adaptive Server for very large databases, disk and cache issues, and the effects of locking and cursors on performance.
- The Utility Programs manual for your platform – documents the Adaptive Server utility programs, such as isql and bcp, which are executed at the operating system level.
- *Error Messages and Troubleshooting Guide* – explains how to resolve frequently occurring error messages and describes solutions to system problems frequently encountered by users.
- *Component Integration Services User's Guide* – explains how to use the Adaptive Server Component Integration Services feature to connect remote Sybase and non-Sybase databases.
- *Java in Adaptive Server Enterprise* – describes how to install and use Java classes as datatypes and user-defined functions in the Adaptive Server database.
- *Using Sybase Failover in a High Availability System* – provides instructions for using Sybase's Failover to configure an Adaptive Server as a companion server in a high availability system.

- *Using Adaptive Server Distributed Transaction Management Features* – explains how to configure, use, and troubleshoot Adaptive Server DTM Features in distributed transaction processing environments.
- *XA Interface Integration Guide for CICS, Encina, and TUXEDO* – provides instructions for using Sybase's DTM XA Interface with X/Open XA transaction managers.
- *Adaptive Server Glossary* – defines technical terms used in the Adaptive Server documentation.

Other sources of information

Use the Sybase Technical Library CD and the Technical Library Product Manuals web site to learn more about your product:

- Technical Library CD contains product manuals and technical documents and is included with your software. The DynaText browser (included on the Technical Library CD) allows you to access technical information about your product in an easy-to-use format.

  Refer to the *Technical Library Installation Guide* in your documentation package for instructions on installing and starting Technical Library.

- Technical Library Product Manuals web site is an HTML version of the Technical Library CD that you can access using a standard web browser. In addition to product manuals, you'll find links to the Technical Documents web site (formerly known as Tech Info Library), the Solved Cases page, and Sybase/Powersoft newsgroups.

  To access the Technical Library Product Manuals web site, go to Product Manuals at http://sybooks.sybase.com.

Sybase certifications on the web

Technical documentation at the Sybase web site is updated frequently.

❖ **For the latest information on product certifications and/or the EBF Rollups:**

1 Point your web browser to Technical Documents at http://techinfo.sybase.com.

2 In the Browse section, click on What's Hot.

3 Select links to Certification Reports and EBF Rollups, as well as links to Technical Newsletters, online manuals, and so on.

❖ **If you are a registered SupportPlus user:**

1 Point your web browser to Technical Documents at http://techinfo.sybase.com.

2 In the Browse section, click on What's Hot.

3 Click on EBF Rollups.

   You can research EBFs using Technical Documents, and you can download EBFs using Electronic Software Distribution (ESD).

4 Follow the instructions associated with the SupportPlus^{SM} Online Services entries.

❖ **If you are not a registered SupportPlus user, and you want to become one:**

You can register by following the instructions on the Web.

To use SupportPlus, you need:

1 A Web browser that supports the Secure Sockets Layer (SSL), such as Netscape Navigator 1.2 or later

2 An active support license

3 A named technical support contact

4 Your user ID and password

❖ **Whether or not you are a registered SupportPlus user:**

You may use Sybase's Technical Documents. Certification Reports are among the features documented at this site.

1 Point your web browser to Technical Documents at http://techinfo.sybase.com

2 In the Browse section, click on What's Hot.

3 Click on the topic that interests you.

Conventions

This manual uses the following style conventions:

- Commands you should enter exactly as shown are given in bold Courier font:

```
isql -Usa -Pshobeen -Sgoby
```

- Words you should replace within a command line with the appropriate value for your installation are shown in the following bold, italicized font:

```
isql -Usa -Ppassword -Sserver_name
```

- Within text, commands you should enter are in regular text and enclosed in quotation marks:

  Exit **isql** by entering "exit" at the prompt.

- Prompts are shown in a regular Courier font:

  ```
  d:\sybase\bin
  ```

- Within text, the names of files and directories appear in italic:

  Use the *\data\master.dat* file.

- The names of utilities, procedures, commands, and scripts appear in the following font:

  sp_revokelogin

Table 2 lists the conventions for syntax statements in this manual:

Table 2: SQL syntax conventions

Key	Definition
command	Command names, command option names, utility names, utility flags, and other keywords are in bold.
variable	Variables, or words that stand for values that you fill in, are in *italic*.
{ }	Curly braces indicate that you choose at least one of the enclosed options. Do not include braces in your option.
[ ]	Brackets mean choosing one or more of the enclosed options is optional. Do not include brackets in your option.
( )	Parentheses are to be typed as part of the command.
|	The vertical bar means you can select only one of the options shown.
,	The comma means you can choose as many of the options shown as you like, separating your choices with commas to be typed as part of the command.

Terms

The following terms appear repeatedly throughout this book. For more detailed information about these and other terms, see the *Adaptive Server Glossary*.

- *System Administrator* – refers to the person responsible for Adaptive Server administration. This person may be different from the person responsible for Windows NT administration.
- *d:\sybase* – is given as an example of the Sybase installation directory.
- *Text editor* – refers to an ASCII text editor or any editor that can save files to text format.

If You Need Help

Each Sybase installation that has purchased a support contract has one or more designated people who are authorized to contact Sybase Technical Support. If you cannot resolve a problem using the manuals or online help, please have the designated person contact Sybase Technical Support or the Sybase subsidiary in your area.

CHAPTER 1

Overview of Adaptive Server Enterprise

Adaptive Server Enterprise for Windows 95, Windows 98 and Windows NT is a full-featured Adaptive Server that runs under the Windows 95, Windows 98 and Windows NT operating system in the Windows environment.

Note The instructions in this book assume that Adaptive Server is running. For information about installing and starting Adaptive Server, see *Adaptive Server Enterprise Installation Guide for Windows NT*.

This chapter gives an overview of how to configure Adaptive Server and the steps you need to take to customize it for your use.

Topics covered are:

About Adaptive Server

Adaptive Server performs data management and transaction functions, independent of client applications and user interface functions.

Adaptive Server also:

- Manages multiple databases and multiple users
- Keeps track of the data’s location on disks
- Maintains the mapping of logical data description to physical data storage
- Maintains data and procedure caches in memory

Adaptive Server uses auxiliary programs to perform dedicated tasks:

- Backup Server manages database loads, dumps, backups, and restores.
- Adaptive Server Enterprise Monitor Historical Server obtains performance data from Monitor Server and saves the data in files for use at a later time.
- XP Server stores the extended stored procedures (ESPs) that allow Adaptive Server to run operating-system level commands.

System-Specific Issues

Adaptive Server runs on a variety of hardware and operating system platforms. System-specific issues do not affect the basic functionality of Adaptive Server, but there are differences among platform implementations. These differences may include:

- Adaptive Server configuration
- Changes to the Windows NT operating system that enable or enhance Adaptive Server performance
- Adaptive Server features that are available only on Windows NT
- The structure of entries in the *sql.ini* file
- Options for selecting database devices
- Operating system commands or utilities that simplify or automate routine system administration tasks
- Operating system utilities for monitoring Adaptive Server performance

System-specific issues are described in this document. For more information, see *Adaptive Server Enterprise Installation Guide for Windows NT.*

New Functionality in Adaptive Server Enterprise Version 12.0

Adaptive Server version 12.0 provides the following new functionality:

- Use of the Unicode™-based conversion mechanism offered by the Unicode Infrastructure Library. You can add the new character sets by adding a new external table. All existing Sybase-supported character sets are included. For more information, see the *Adaptive Server Enterprise Installation Guide for Windows NT*.
- The **sortkey** and **compare** functions, which provide sophisticated collation support for companies that use languages other than U.S. English. For more information, see the *Adaptive Server Enterprise Installation Guide for Windows NT*.

Support for High-Availability Products

Adaptive Server is compatible with high-availability packages for several platforms and operating systems, such as the Compaq On-Line Recovery Server.

You can access the configuration procedures for these high-availability packages from the Sybase World Wide Web site.

To view the high-availability setup procedures:

1. Use a Web browser to access the Sybase World Wide Web site at the following address:

   http://www.sybase.com

2. Click the Technical Support button.
3. Navigate to the Technical Information Library.
4. Type “High Availability” in the Search utility, and click Search.

The Search utility generates a list of titles for Technical Notes that contain high-availability configuration procedures. See the titles that include “Configuring Sybase SQL Server for High Availability” and a reference to Windows NT.

Languages Other Than U.S. English

Many of the configuration tasks described in this manual require the use of the Server Config utility.

If you are running Server Config in a language other than U.S. English, make sure that any input you provide uses a character set that is supported by the us_english character set.

Note The us_english character set does not support accent marks, such as tildes (~) and umlauts (ü). This prevents Server Config from supporting the character sets that use these characters.

For more information about languages, character sets, and sort orders, see the *Adaptive Server Enterprise Installation Guide for Windows NT*.

CHAPTER 2

Beginning Adaptive Server Configuration

When you install or upgrade Adaptive Server, it includes some default parameter settings and a few of its auxiliary programs.

After installing and testing this “default” Adaptive Server, you can configure it to your system’s needs and install other optional features.

Topics covered are:

For information about configuring languages, character sets, and sort orders, as well as optional features, see “How to Use This Book” on page vii.

Adaptive Server Default Configuration

After installation, Adaptive Server default settings are as listed in Table 2-1. You might need to configure these settings to suit your computer and database needs.

Table 2-1: Defaults for Adaptive Server parameter settings

Item	Default Value
Name	*AdaptiveServername*
Network support	Named Pipes, Windows Sockets (TCP/IP)
Pipe name	*\pipe\sybase\’uery*
Socket number	5000
Command line options	None
Error log path	*d:\sybase\install\errorlog*
Event logging	Not configured
International Support (Localization) - Language - Character set - Sort order	 us_english cp850 Binary ordering
Login security mode	Standard

Table 2-2 lists the default settings for the Backup Server, Monitor Server, and XP Server. For more information about these servers, see “About Adaptive Server” on page 2.

Table 2-2: Defaults for the Backup, Monitor, and XP servers

Server	Item	Default Value
Backup Server	Name	*AdaptiveServername*_BS
	Network support	Named Pipes, Windows Sockets (TCP/IP)
	Pipe name	*\pipe\sybase\backup*
	Socket number	5001
	Error log path	*d:\sybase\install\backup.log*
Monitor Server	Name	*AdaptiveServername*_MS
	Network support	Named Pipes, Windows Sockets (TCP/IP)
	Pipe name	*\pipe\sybase\monitor*
	Socket number	5002
	Error log path	*d:\sybase\install\ms.log*

Server	Item	Default Value
XP Server	Name	*AdaptiveServername*_XP
	Network support	Named Pipes, Windows Sockets (TCP/IP)
	Pipe name	*\pipe\sybase\xp*
	Socket number	5003
	Error log path	N/A

Starting Server Config for Adaptive Server

To change configuration settings for Adaptive Server, use the Server Config utility. You can run this program in one of two ways:

- The Server Config utility from within Windows NT

  To run this utility from the Windows NT command prompt, run **syconfig.exe.**

- The **sp_configure** procedure from within **isql**

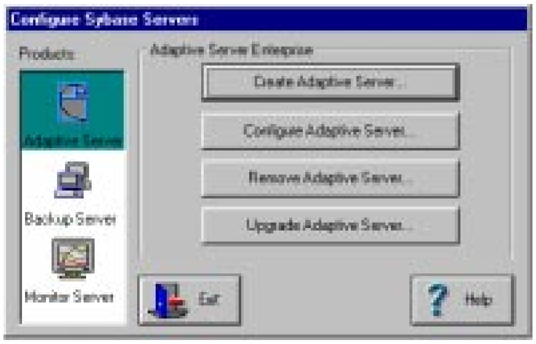
  Use the **sp_configure** procedure, which appears in several places in this manual, to quickly and easily change single parameters and values. For more information, see **sp_configure** in the *Adaptive Server Reference Manual*.

This manual walks you through Adaptive Server configuration through the Server Config utility.

To start Server Config:

1. Select Programs from the Start menu.
2. Choose your Sybase program group.
3. Choose Server Config.

   The Configure Sybase Servers dialog box appears:


Configure Sybase Servers
Products
Adaptive Server
Backup Server
Monitor Server
Adaptive Server Enterprise
Create Adaptive Server...
Configure Adaptive Server...
Remove Adaptive Server...
Upgrade Adaptive Server...
Exit
Help

4. Continue configuration for the server that you want to configure:
   - For more information on how to configure Adaptive Server, see “Configuring Adaptive Server” on page 12
   - For more information on how to configure Backup Server, see “Configuring Backup Server” on page 16

- For more information on how to configure Monitor Serve, see "Configuring Monitor Server" on page 18

5 When you have completed the necessary configuration changes, click Exit to quit Server Config.

Configuring Adaptive Server

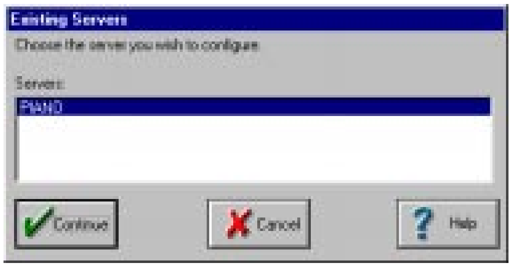
To change the Adaptive Server configuration, including its auxiliary programs and options:

1 Start Server Config.

For instructions on starting this utility, see “Starting Server Config for Adaptive Server” on page 10.

2 Click the Adaptive Server icon, and click Configure Adaptive Server from the Configure Sybase Servers dialog box.

The server names appear in the Existing Servers dialog box:



Existing Servers

Choose the server you wish to configure

Servers:

PIANO

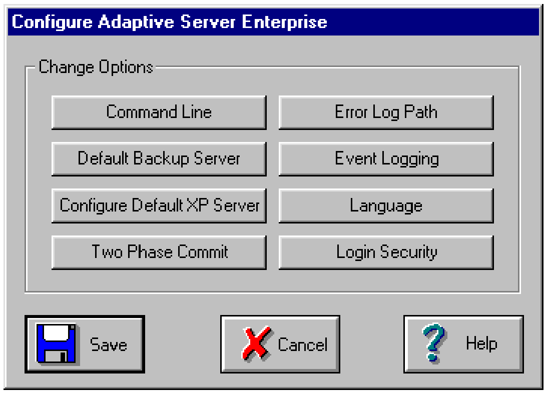
3 Select the name of the server to configure, and click Continue.

The Enter System Administrator Password dialog box appears.

4 Type the login name and password of an Adaptive Server user with System Administrator privileges, and click Continue.

5 Click Yes if the Adaptive Server is not running, and Server Config asks you if you want to start it.

The Configuring Adaptive Server Enterprise dialog box appears.



6 Select the option to be configured from the Change Options set of buttons:

- Command Line – see “Setting Adaptive Server Parameters” on page 13
- Default Backup Server – see “Changing the Default Backup Server” on page 14
- Default XP Server – see “Changing the Default XP Server” on page 15
- Two Phase Commit – see the *Adaptive Server Enterprise Installation Guide for Windows NT*.
- Error Log Path – see “Setting Error Log Paths” on page 60
- Event Logging – see “Enabling and Disabling NT Event Logging” on page 64
- Language – see the *Adaptive Server Enterprise Installation Guide for Windows NT*
- Login Security – see “Configuring Login Security” on page 113

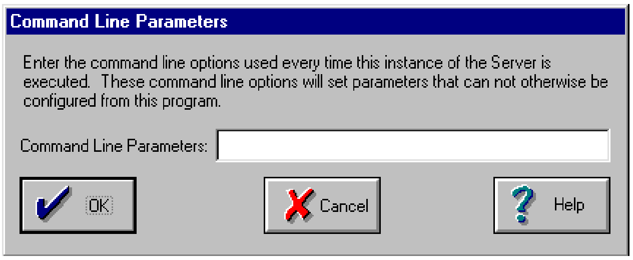
Setting Adaptive Server Parameters

When you start Adaptive Server, you can configure the server to use certain configuration parameters that are not accessible through **isql.**

To set these configuration parameters:

1 Click Command Line from the Change Options box on the Configuring Adaptive Server Enterprise dialog box.

The Command Line Parameters dialog box appears.



Enter the command line options used every time this instance of the Server is executed. These command line options will set parameters that can not otherwise be configured from this program.

Command Line Parameters:

2 Type in parameters and values that you want to set for Adaptive Server.

Type these parameters as you would at the command line. However, be sure to omit the command itself and any parameters that might vary.

3 Click OK to return to the Configure Adaptive Server Enterprise dialog box.

4 When you have completed the necessary configuration changes, click Exit to quit Server Config.

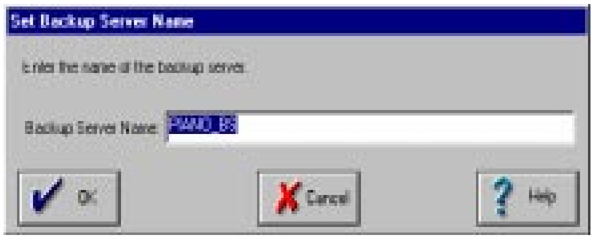
Changing the Default Backup Server

During backup or recovery, the **dump** or **load** command uses the Backup Server named in the configuration for the selected Adaptive Server. You can name a different default Backup Server through the Adaptive Server configuration.

To name a different Backup Server to use as the default:

1 Click Default Backup Server from the Change Options buttons.

The Set Default Backup Server Name dialog box appears.



Enter the name of the backup server.

Backup Server Name: PIANO_BS

2 Type the name of the Backup Server as the default, and click OK.

For information about naming and configuring Backup Server, see "Configuring Backup Server" on page 16.

3 Click Save to return to the Configuring Adaptive Server Enterprise dialog box.

4 When you have completed the necessary configuration changes, click Exit to quit Server Config.

Changing the Default XP Server

XP Server provides the extended stored procedures available through Adaptive Server.

When you install Adaptive Server, the program defines XP Server using the Adaptive Server name as a basis for the filename. For example, XP Server for an Adaptive Server named PIANO is named PIANO_XP.

You can change the configuration for the default XP Server for a particular Adaptive Server. See "Sybmail and Extended Stored Procedures" on page 124.

Configuring Backup Server

Backup Server performs all Adaptive Server backup and recovery operations (**dump** and **load**).

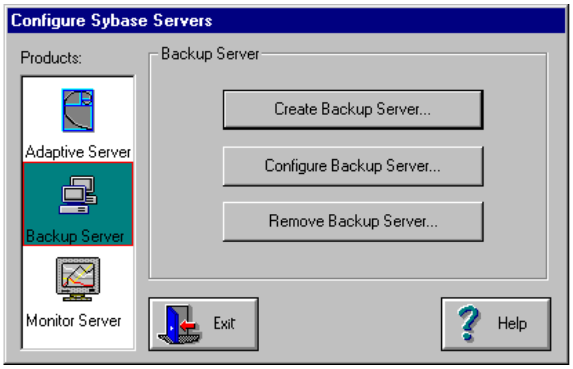
When you install Adaptive Server, the program defines Backup Server using the Adaptive Server name as a basis for the filename. For example, Backup Server for an Adaptive Server named PIANO is named PIANO_BS.

To change the configuration for a Backup Server:.

1 Start Server Config.

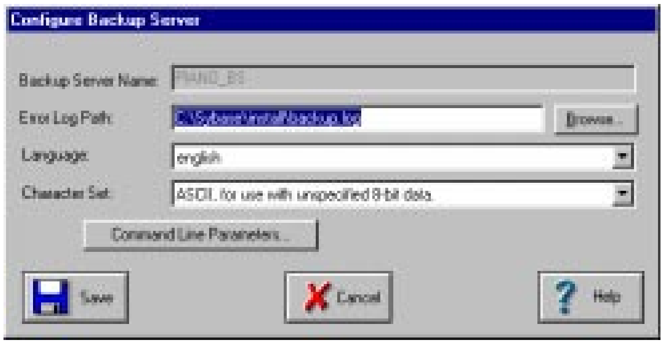
For instructions on starting this utility, see “Starting Server Config for Adaptive Server” on page 10.

2 Click the Backup Server icon, and click Configure Backup Server from the Configure Sybase Servers dialog box.



3 Select the name of the server to configure from the Existing Servers dialog box, and click Continue.

The Configure Backup Server dialog box appears.



Backup Server Name: PIANO_BS

Error Log Path: C:\Sybase\install\backup.log

Language: english

Character Set: ASCII, for use with unspecified 8-bit data

4 Change the path indicated in the Error Log Path area, if necessary.

For more information about the error log, see Chapter 5, “Logging Error Messages and Events”.

5 Change the language indicated in the Language area that Backup Server will use for its messages, if necessary.

For more information about languages, see the *Adaptive Server Enterprise Installation Guide for Windows NT*.

6 Change the server’s character set in the Character Set area, if necessary.

For more information about character sets, see the *Adaptive Server Enterprise Installation Guide for Windows NT*.

7 Click Save to return to the Configure Sybase Servers dialog box.

8 When you have completed the necessary configuration changes, click Exit to quit Server Config.

Configuring Monitor Server

Monitor Server is an Open Server™ application that obtains statistics on Adaptive Server performance by monitoring its shared memory. You can view these statistics from the Monitor Viewer in Sybase Central™.

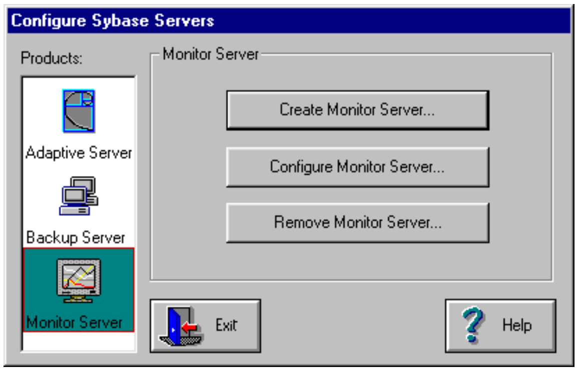
Database administrators can use Monitor Server to examine server statistics using a graphical client/server tool. Statistics are available for:

- Memory allocation
- Network traffic
- CPU use
- Locking status by process
- Data and procedure cache use
- Disk I/O volume and average completion time by device
- Transaction rates

To change the configuration for Monitor Server:

1 Start Server Config.

For instructions on starting Server Config, see “Starting Server Config for Adaptive Server” on page 10.

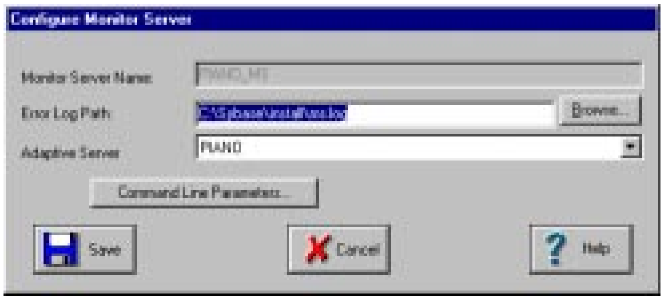


2 Click the Monitor Server icon, and click Configure Monitor Server from the Configure Sybase Servers dialog box.

The Existing Servers dialog box appears.

3 Click the name of the Monitor Server you want to configure, and click Continue.

The Configure Monitor Server dialog box appears.



Configure Monitor Server

Monitor Server Name: PIANO_MS

Error Log Path: C:\Sybase\install\ms.log

Adaptive Server: PIANO

4 Change the error log path, if necessary.

5 Change the Adaptive Server Name entry to the Adaptive Server name to be monitored. The Monitor Server name changes automatically.

6 Click on the Command Line Parameters button to change the default parameters.

For more information on default command line parameters, see “Setting Adaptive Server Parameters” on page 13.

7 Click Save to return to the Configure Sybase Servers dialog box.

8 When you have completed the necessary configuration changes, click Exit to quit Server Config.

For more information about configuring Monitor Server, see the *Adaptive Server Enterprise Monitor Server User’s Guide.*

Supporting Access to Large Memory

To support access to 2GB of memory, use **isql** to set the starting virtual memory address with **sp_configure**, for example:

```
sp_configure "shared memory starting address", 23662592
```

Be sure to reboot your computer to put the new value into effect.

Note Do not set Monitor Server to use most of the available virtual address space. This access may limit Monitor Server functionality.

For instructions on displaying the latest information about large memory and Windows NT, see “Support for High-Availability Products” on page 5.

For more information about shared memory, see *Adaptive Server Enterprise Installation Guide for Windows NT*.

CHAPTER 3

Setting Up Communications Across the Network

Adaptive Server can communicate with other Adaptive Servers, Open Server applications, and client software across a network. Clients can communicate with one or more servers, and servers can communicate with other servers via remote procedure calls.

This chapter describes the connection process, the kinds of connections, and how to configure Adaptive Server to use these connections.

Topics covered are:

For instructions on using Server Config to change the values that it can access, see Chapter 2, “Beginning Adaptive Server Configuration”.

Adaptive Server on Windows NT supports network connections using the Named Pipes, Sockets (TCP/IP), and IPX/SPX protocols. The default Adaptive Server uses TCP/IP and Named Pipes, since Named Pipes is always installed with Windows NT.

Two files control how clients find servers and drivers:

- The *sql.ini* file lists the server names, their network addresses, and the Net-Library driver to use to establish a connection.
- The library file, *libtcl.cfg*, lists the installed Net-Library drivers that are available to support each protocol (connection).

These files, which reside on both server and client machines, enable each Sybase product to find the other Sybase servers that are on the network. The installation program automatically creates, verifies, and appends these configuration files when you install Adaptive Server.

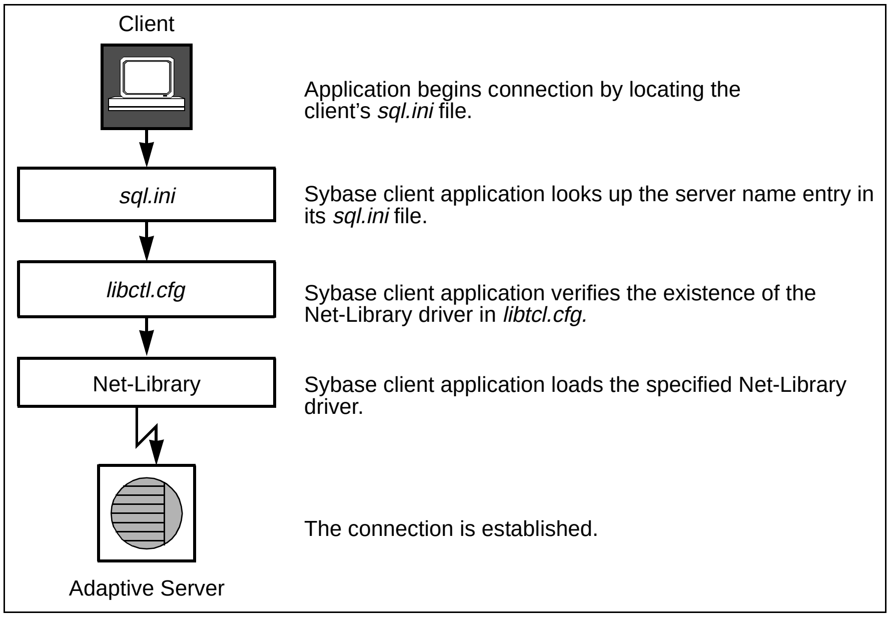
How Clients Connect to Adaptive Server

Client software performs the following steps to connect to Adaptive Server:

1. Determines the name of the Adaptive Server by finding the value of the DSQUERY environment variable, by using a command line option, or by defaulting to the value *d:\sybase*.
2. Looks in the *sql.ini* file for an entry whose name matches the name of the server. If it cannot find a matching entry, the connection fails.
3. Looks in the *libtcl.cfg* file for an entry that matches the Net-Library driver name associated with the server entry in the *sql.ini* file. If the application cannot find such an entry, the connection fails.
4. Loads the specified Net-Library driver.
5. Uses the network connection information provided by the *sql.ini* file to connect to the server.

Figure 3-1 summarizes the client connection process.

Figure 3-1: Connecting to Adaptive Server



Application begins connection by locating the client's *sql.ini* file.

Sybase client application looks up the server name entry in its *sql.ini* file.

Sybase client application verifies the existence of the Net-Library driver in *libtcl.cfg.*

Sybase client application loads the specified Net-Library driver.

The connection is established.

How Adaptive Server Listens for Client Connections

Adaptive Server uses the *sql.ini* file to determine the address at which it should listen for clients. When you start Adaptive Server, it performs the following steps:

1. Determines the server name to use, usually by finding the value of the DSLISTEN environment variable or by using a command line option.
2. Looks in the *sql.ini* file for an entry that matches the specified server name.
3. Looks in the *libtcl.cfg* file for an entry that matches the Net-Library driver name associated with the server entry in the *sql.ini* file.
4. Loads the specified Net-Library driver.
5. Uses the information from the MASTER entry in the *sql.ini* file to determine the address at which it should listen for client connection requests.

How a Client Accesses Adaptive Server

The installation program provides a default *sql.ini* file in Adaptive Server. The file has MASTER and QUERY entries that use both the Named Pipes and Sockets (TCP/IP) drivers for all servers that were installed.

Enabling Client Access to a Server

To enable a client to access a server on the network, create a *sql.in*i file on the client. In that file, include entries for all servers the client needs to access.

To create a new *sql.ini* file, see "Changing the Server Entries in sql.ini" on page 25.

Changing the Server Entries in *sql.ini*

To edit an existing *sql.ini* file on the server machine, or to create a new file on the client machine, use the Directory Services Editor utility, **dsedit**.

For more information about the components of a *sql.ini* file, see "Components in the sql.ini File" on page 28.

For more information about using **dsedit**, see *Utility Programs for Windows 95, Windows 98, and Windows NT*.

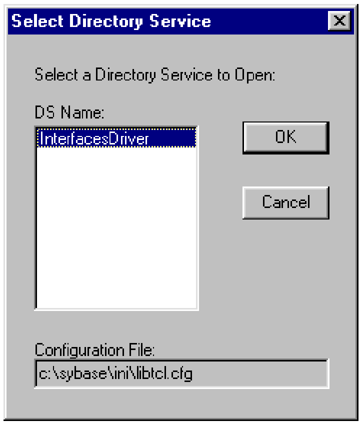
For general information about the *sql.ini* file, see the *Open Client/Server Configuration Guide for Desktop Platforms*.

To start **dsedit**, select it either from the Sybase program group or from the Utilities group in Sybase Central™.

To add an Adaptive Server to the *sql.ini* file:

1 Select Programs from the Start menu, select Sybase, and select **dsedit**.

The Select Directory Service dialog box appears.



Select a Directory Service to Open:

DS Name:

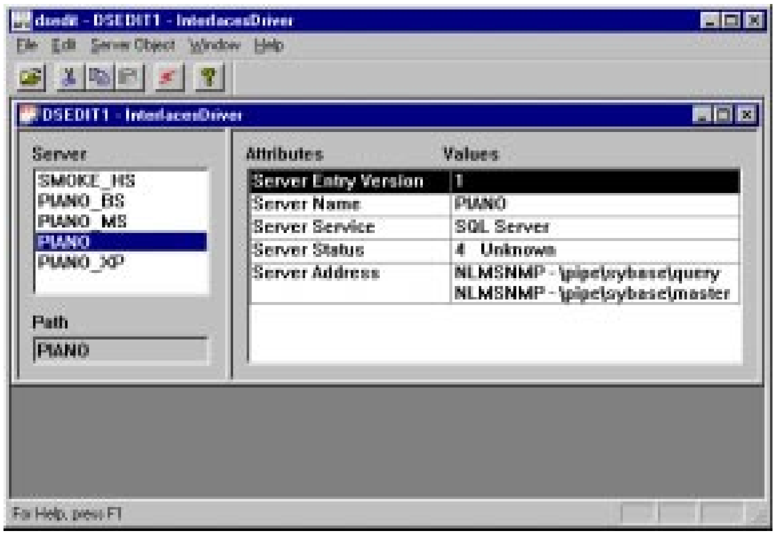
InterfacesDriver

Configuration File:

c:\sybase\ini\libtcl.cfg

2 Select a driver from the DS Name list, and click OK.

The DSEDIT - Interfaces Driver dialog box appears.


dsedit - DSEDIT1 - InterfacesDriver
File
Edit
Server Object
Window
Help
DSEDIT1 - InterfacesDriver
For Help, press F1

Server

SMOKE_HS
PIANO_BS
PIANO_MS
PIANO
PIANO_XP

Path

PIANO

Attributes	Values
Server Entry Version	1
Server Name	PIANO
Server Service	SQL Server
Server Status	4 Unknown
Server Address	NLMSNMP - \pipe\sybase\query NLMSNMP - \pipe\sybase\master

3 Select Server Object menu, and select Add.

The Input Server Name dialog box appears.

4 Type the name of the server to add, and click OK.

For information about valid server names, see “Server Name” on page 28.

5 Select the new server name, which you have just added, from the Server list.

Steps 6-10 describe how to enter the server's address:

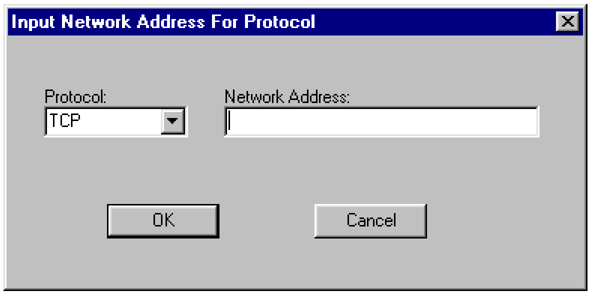
6 Select Server Address from Attributes box on the Interfaces Driver window.

7 Select the Server Object menu and select Modify Attribute.

The Network Address Attribute dialog box appears.

8 Click Add.

The Input Network Address For Protocol dialog box appears:



Input Network Address For Protocol

Protocol: TCP

Network Address:

9 Choose the appropriate protocol from the drop-down list, enter the network address in the Network Address text box, and click OK.

For information about protocols, see "Network Driver" on page 29.

For information about the formats of network addresses required by the different protocols, see "Server Address" on page 29.

The Network Address Attribute dialog box reappears.

10 Click OK.

The **dsedit** utility creates MASTER and QUERY entries for the server. In the *sql.ini* file, the client ignores the MASTER entry.

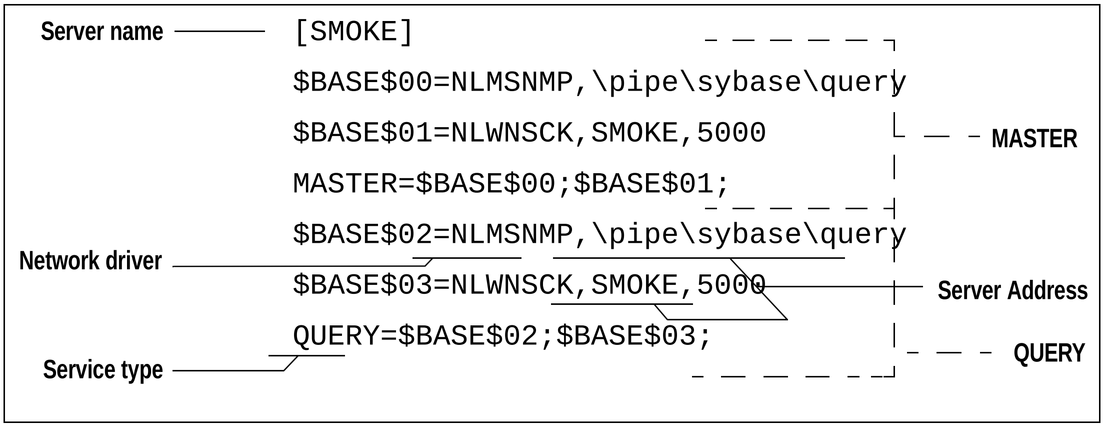
11 Exit **dsedit**.

Components in the *sql.ini* File

This section provides useful background information for editing an *sql.ini* file.

Figure 3-2 illustrates the basic components of an entry in the *sql.ini* file. The sections that follow the figure describe components.

Figure 3-2: Components of the sql.ini file



```
[SMOKE]
$BASE$00=NLMSNMP,\pipe\sybase\query
$BASE$01=NLWNSCK,SMOKE,5000
MASTER=$BASE$00;$BASE$01;
$BASE$02=NLMSNMP,\pipe\sybase\query
$BASE$03=NLWNSCK,SMOKE,5000
QUERY=$BASE$02;$BASE$03;
```

Server Name

The server name is the name of the Adaptive Server to which clients will connect. Use the following rules to create an acceptable server name:

- Server names can be no more than 11 characters long. However, if you installed Adaptive Server on a FAT (file allocation table) partition, limit the server name to 8 characters.
- The initial character of a server name must be a letter (a–z, A–Z). The characters that follow can be letters, numbers, the underscore character (_), the pound sign (#), the at sign (@), or the dollar sign ($).
- The name cannot contain a period (.), a slash (/), a backslash (\), an accented letter, a character from a Japanese character set, or any other character that is invalid for Windows NT file names.
- Adaptive Server names are not case sensitive. For example, “PRODUCTION,” “Production,” and “production” are interpreted as the same server name.

Network Driver

The network driver specifies the name of the Net-Library driver to use for the connection. The driver name must correspond to a valid entry in the library (*libtcl.cfg*) file, which is located in the *ini* subdirectory of the Sybase installation directory.

The following example shows three driver entries in a *libtcl.cfg* file:

```
NLMSNMP=NLMSNMP Named Pipes Driver
 NLWNSCK=NLWNSCK WinSock TCP/IP Driver
 NLNWLINK=NLNWLINK NWLink SPX/IPX Driver
```

Note As drivers are added or removed, you can edit the *libtcl.cfg* file with a text editor or with the **ocscfg.exe** utility, located in the *bin* subdirectory of the Sybase installation directory.

Service Type

The Service Type defines the Adaptive Server's service. The two service types are MASTER and QUERY:

- MASTER defines the service that Adaptive Server uses to listen to login requests from clients. This type defines a server machine.

  A MASTER entry is required only if you plan to use your computer as a server. It is not required in a *sql.ini* file for a computer that is running clients only.

- QUERY represents the service that a client application uses to log into Adaptive Server. This type defines a client machine.

  A QUERY entry is required if you plan to use your computer to access a server. In general, since even dedicated servers need access to other servers, a QUERY entry is always required.

Server Address

This value is the address at which Adaptive Server listens for client connections. The address requires the following information:

- Address Format

- IP Address
- Named Pipes Format
- Windows Sockets Format
- NWLink IPX/SPX Format

Address Format

The format of the server address depends on the network driver used by Adaptive Server.

The format for the server address can be:

- Named Pipes Format
- Windows Sockets Format
- NWLink IPX/SPX Format

Use the following guidelines to define your server address:

- Some formats require a port, or socket number. Port numbers for MASTER and QUERY entries must be the same on server and client. For example, if a server is listening on 5000, the client workstation must be connecting on 5000.
- The server usually controls the port number, which means that you specify the same port number in the client's *sql.ini* file as that specified in the *sql.ini* file for the server to which it will connect.
- Port addresses must be unique to each server. The port address is determined by the port number provided in the *sql.ini* file in conjunction with the IP address.
- By default, the port number for Adaptive Server is 5000, for Backup Server, it is 5001, and for Monitor Server, it is 5002.

Note Two Adaptive Servers on different computers can use the same port number because their IP addresses are different.

IP Address

If you know a computer’s IP address as well as its name, specify the IP address in the *sql.ini* file to ensure that the computer can be found on the network.

For example, the following entry, which uses Named Pipes, specifies a remote server's computer name and requires name resolution:

```
NLMSNMP,\\SMOKE\pipe\sybase\'uery
```

The following entry uses a remote server's IP address and does not require name resolution:

```
NLMSNMP,\\130.214.60.230\pipe\sybase\'uery
```

Named Pipes Format

For the Named Pipes protocol, the network address consists of the unique pipe name for the server.

Use the following guidelines to create acceptable pipe names.

- Valid pipe names begin with *\pipe* and follow the same naming restrictions as MS-DOS file names. The default pipe name for Adaptive Server is *\pipe\sybase\query*.
- To avoid conflict, always use unique pipe names of the same "length" (levels) for all Sybase products on your computer. For example, you might select *\pipe\sybase\query* for Adaptive Server and *\pipe\backup\query* for Backup Server.
- Do not use pipe names such as *\pipe\sql* and *\pipe\sql\query*, because they do not ensure uniqueness.
- When adding a network entry to access a server on a remote network computer, such as on a client, preface the pipe name for the QUERY service with:

  ```
  \\machine_name
  ```

  where *machine_name* is the name of the computer that runs the server.

Warning! Server pipes must be local. Do not add *\\machine_name* if you are configuring a network entry for a server on a local computer. And, do not preface the pipe name with this prefix when entering connection information for the MASTER service. If you include this prefix, you cannot restart Adaptive Server.

Windows Sockets Format

For the Windows Sockets protocol, the server address consists of the TCP/IP host name or IP address of the NT computer and a unique socket for the Adaptive Server, separated by a comma.

Keep the following guidelines in mind when creating the address:

- The TCP/IP host name is case sensitive. For example, a possible entry for a TCP/IP host named “CENTAUR” is “CENTAUR, 5000”.
- Adaptive Server uses the default socket number of 5000 to listen to connections from client workstations. Be sure to select a different socket number if another application on your computer already uses socket 5000.
- Valid socket numbers for Adaptive Server range from 1025 to 65535, in integers.

Increasing Windows Sockets Connections

To support more than 64511 Windows Sockets (TCP/IP) connections to Adaptive Server, you may need to use the NT Registry to increase the maximum number of sockets connections available on the server.

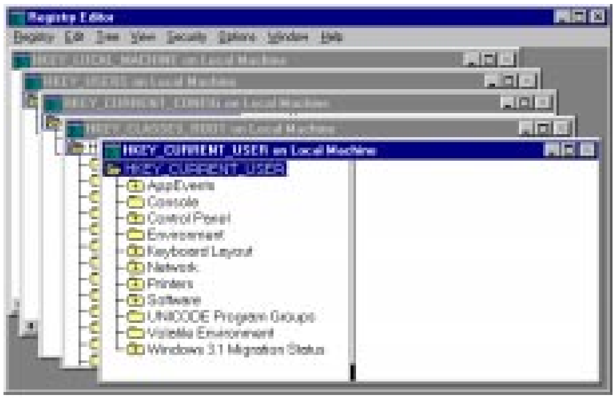
Warning! Do not modify a Registry value unless you are an NT administrator and are familiar with the **regedt32** utility.

See your NT operating system documentation for information on using **regedt32**.

To modify an existing TcpNumConnections value:

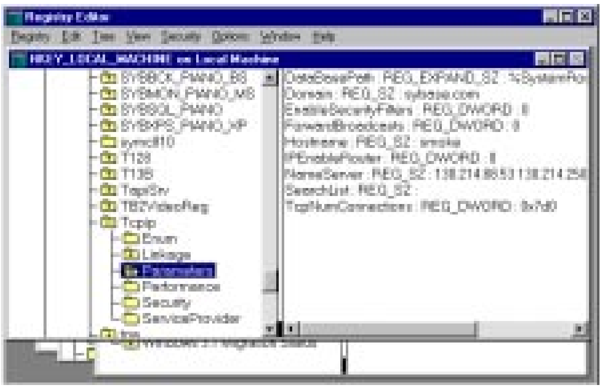
1. Log into Windows NT using an account with NT administrator privileges.

2 Start the **regedt32** utility from the Windows NT program group.


Registry Editor
Registry Edit Tree View Security Options Window Help
HKEY_LOCAL_MACHINE on Local Machine
HKEY_USERS on Local Machine
HKEY_CURRENT_CONFIG on Local Machine
HKEY_CLASSES_ROOT on Local Machine
HKEY_CURRENT_USER on Local Machine
HKEY_CURRENT_USER
AppEvents
Console
Control Panel
Environment
Keyboard Layout
Network
Printers
Software
UNICODE Program Groups
Volatile Environment
Windows 3.1 Migration Status

3 Select the Registry window HKEY_LOCAL MACHINE.

4 Open the Registry key HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\Tcpip\Parameters.



```
DataBasePath : REG_EXPAND_SZ : %SystemRo
Domain : REG_SZ : sybase.com
EnableSecurityFilters : REG_DWORD : 0
ForwardBroadcasts : REG_DWORD : 0
Hostname : REG_SZ : smoke
IPEnableRouter : REG_DWORD : 0
NameServer : REG_SZ : 138.214.88.53 138.214.250
SearchList : REG_SZ :
TcpNumConnections : REG_DWORD : 0x7d0
```

5 If the TcpNumConnections value exists, go to step 6.

If the value does not exist, add and configure it by completing the steps under “To add a TcpNumConnections value”.

6 Double-click the value.

7 In the DWORD Editor dialog box, select the Decimal option.

8 In the Data text box, enter the maximum number of connections to support.

9 Click OK to return to the Registry key dialog box.

10 If you have completed your tasks in **regedt32**:

- a Select Exit from the Registry menu to quit **regedt32**.
- b Reboot your computer.

To add a TcpNumConnections value:

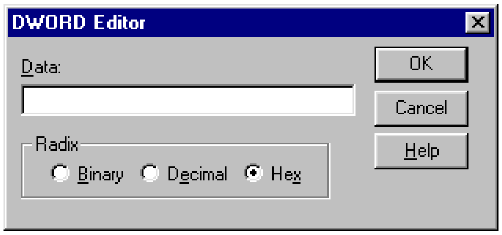
1 Complete the Add Value dialog box as follows:

Value Name – TcpNumConnections

Data Type – select REG_DWORD from the drop-down list.

2 Click OK.

The utility displays a DWORD Editor dialog box similar to the one that follows:



Radix: ○ Binary ○ Decimal ● Hex

3 Complete the DWORD Editor dialog box as follows:

Data – enter the maximum number of TCP connections for the computer.

Radix – select the Decimal option button.

4 Click OK.

The utility adds the new value to the Registry key.

5 If you have completed your tasks in **regedt32**:

- a Choose Exit from the Registry menu to quit **regedt32**.
- b Reboot your computer.

Using Multiple TCP/IP Network Interface Cards

When client workstations use multiple TCP/IP network interface cards, the NT system administrator must edit the *lmhosts* file on the Windows NT server to accept connections from the clients.

Use the following guidelines to correctly enter the card information.

- There must be one entry for each network card.
- Each address must be unique.
- The entries in the *lmhosts* file match those in the *sql.ini* file.

For example, assume that a server named BALCLUTHA has three cards. Without an *lmhosts* entry and separate entries in *sql.ini*, the server listens on socket BALCLUTHA,5000 for all three cards. To provide unique addresses, set up *lmhosts* as follows:

```
130.214.10.248    NT0
130.214.11.248    NT1
130.214.12.248    NT2
```

In the *sql.ini* file, add entries for both QUERY and MASTER:

```
[BALCLUTHA]
query=NT0,5000
master=NT0,5000
query=NT1,5000
master=NT1,5000
query=NT2,5000
masterNT2,5000
```

Controlling the Connection Timeout

When an **isql** connection remains idle for several minutes, the next query may result in this error message:

```
Attempt to initiate a new SQL Server operation with
results pending.
```

This problem occurs when you use the Windows Sockets protocol, and you have a small value for the NT TcpKeepTries value. To correct this problem, you must increase the value in the NT TcpKeepTries value.

Warning! Do not modify Registry values unless you are an NT administrator and you are familiar with the **regedt32** utility. See the NT operating system documentation for information on using **regedt32**.

To increase the TcpKeepTries value:

1 Start the **regedt32** utility, and display the Parameters values.

If necessary, see “Increasing Windows Sockets Connections” on page 32 for information on starting the **regedt32** utility.

2 Double-click the TcpKeepTries value.

3 Change the data value to at least 20, and choose OK.

4 If you have completed your tasks in **regedt32**:

   a Choose Exit from the Registry menu to quit.

   b Reboot your computer.

NWLink IPX/SPX Format

Before setting up Adaptive Server network support, configure the NWLink IPX/SPX software according to the instructions for your NT operating system. Be sure to specify the correct network number (usually 0) and frame type during the configuration.

The frame type is generally mandated by the frame type of a NetWare file server on the network, usually 802.3. If your network does not use a NetWare file server, make sure all client and server computers use the same frame type.

Available NWLink IPX/SPX Connection Formats

Table 3-1 describes the available connection formats for NWLink IPX/SPX MASTER and QUERY entries.

Table 3-1: Connection information formats for IPX/SPX

Format	Connection Information Syntax	Example
1	*net_number,node_number,socket_number*	00000000,02608CDA1997,83BD
2	*cotmputer_name,socket_number*	piano,83BD
3	*computer_name*	piano

Keep the following items in mind when working with these formats:

- Any of the three formats is acceptable for the MASTER entry.
- Only Format 1 and Format 3 are acceptable for QUERY entries.
- Some formats are not acceptable for accessing a local Adaptive Server.

  For more information, see “Selecting Valid Connection Formats” on page 37.

Finding the Network Number

In Table 3-1, *net_number* is the network number that you specified during the NWLink IPX/SPX configuration.

To find the network number, open the Windows NT Control Panel and open Network. The current network number is the decimal number in the NWLink Transport entry.

Finding the Node Number, Socket Number, and Computer Name

To determine the *node_number*, enter the **net config** command at the Windows NT command prompt. For example:

```
net config workstation
Computer name              \\PIANO
User name                  user1
Workstation active on      NBT_Elnk31 (00A0242EA892)
Software version           Windows NT 4.0
Workstation domain         AMERICAS
Logon domain               AMERICAS
COM Open Timeout (sec)     3600
COM Send Count (byte)      16
COM Send Timeout (msec)    250

The command completed successfully.
```

In the preceding example:

- The *node_number*, which is a 4-byte, hexadecimal number in the connection information string, appears in parentheses; “00A0242E”.
- The *socket_number*, which can be any unused socket number on the computer, in 2-byte, hexadecimal format, appears with the *node_number*; “A892”.
- The *computer_name* can be any unique name on the network. Use the local computer’s name to ensure uniqueness: PIANO

Selecting Valid Connection Formats

The NWLink IPX/SPX connection formats you use depend on whether you want to access Adaptive Server on a local computer or on a remote, network computer.

- When both Adaptive Server and the client program reside on the same computer, a local connection, use a Named Pipes connection.
- If you must use NWLink IPX/SPX for a local connection, follow these guidelines:
    - Use either Format 1 or Format 2 for the MASTER entry.
    - Use only Format 1 for the QUERY entry.

- If Adaptive Server and its clients reside on separate computers, a remote connection, you have two options:
    - Use Format 3 for both the MASTER and QUERY entries.
    - Use either Format 1 or Format 2 for the MASTER entry, but use Format 1 for the QUERY entry.

Sharing Network Configuration Information

There are two ways to share identical network information across multiple systems:

- Create a master Interfaces (*sql.ini*) file.
- Use NT Registry as a directory service.

Creating a Master *sql.ini* File

A master *sql.ini* file contains entries for all Sybase servers on the network. It can be used with every server and client connected to the network. By distributing copies of a master *sql.ini* file, you can ensure that all Sybase products on the network interact with one another.

To maintain consistency in the *sql.ini* files on a network, make the changes to one version of the file, and then copy that file to the rest of the computers on the network. For this task, you can use NT Directory Replication to copy the file to many computers. For more information, see your NT operating system documentation.

Using NT Registry As a Directory Service

Another option is to use the NT Registry as a directory service. Review the following Sybase product arrangements before settling on this method:

- Adaptive Server Enterprise only – you can deploy an application on multiple clients and enter the network information once in the Registry on the Adaptive Server computer without needing to create and maintain a *sql.ini* file on every client.
- Adaptive Server Enterprise and its bundled applications – the client applications that are bundled with Adaptive Server require a *sql.ini* file. Even if you are using the Registry for your own applications, you still need to maintain a *sql.ini* file if users are to connect from any of the Sybase client applications, such as Sybase Central or NetImpact™ Dynamo.

To Use NT Registry As a Directory Service

The following instructions create server name keys under the Registry key specified for “ditbase” in *libtcl.cfg*, in the example in step 2, SOFTWARE\SYBASE\SERVER. It also stores the network information in the keys.

Both the Adaptive Server and client applications look in the Registry for network information before searching the *sql.ini* file.

You'll need both the Open Client/Open Server Configuration and the **dsedit** utilities to complete this task.

To use NT Registry as a Directory Service:

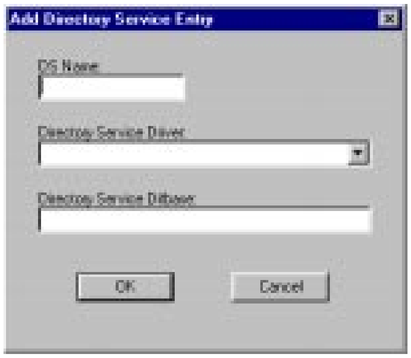
1 Make sure the *ocscfg.dat* file is in your *d:\sybase\bin* directory.

2 Start the OC OS Config Utility.

a Select Programs from the Start menu, choose your Sybase group, and choose OC OS Config Utility.

b Select the Directory Services tab.

c Click Add.



d Type REGISTRY for the DS Name.

e Type LIBDREG for the Directory Service Driver or select it from the drop-down list.

f Type \\machine_name:SOFTWARE\SYBASE\SERVER for the Directory Service Ditbase, where *machine_name* is the name of the computer that stores the network information.

g Click OK. The values you entered appear on the Directory Services dialog box.

You can also use a text editor to add the following lines to the *libtcl.cfg* file:

```
[NT_DIRECTORY]
 REGISTRY=LIBDREG ditbase=\\machine_name:SOFTWARE\SYBASE\SERVER
```

For information about using **ocscfg**, see the *Open Client/Server Configuration Guide for Desktop Platforms*.

3 Start **dsedit**.

   a Select Programs from the Start menu, choose your Sybase group, and choose **dsedit**.

   b In the Select Directory Service dialog box, select Registry from the DS Name list, and click OK.

   c Follow the instructions in “How a Client Accesses Adaptive Server” on page 25 for creating server entries using **dsedit**.

Verifying Server Connections

After you configure your network connections, use the **dsedit** utility to verify that you can connect to a server. **dsedit** includes a network diagnostic utility that checks to see whether a process is listening at the specified address.

You can access this diagnostic utility in one of two ways:

- By choosing Server Object, then Server Ping from the **dsedit** menu, or
- By pressing the Ping (lightening bolt) key on your keyboard.

See Chapter 9, “Troubleshooting Network Connections” , for information about using **dsedit** to test connections.

Configuring ODBC Connections

Some client applications do not connect to Adaptive Server directly through the Open Client™ software, but through the ODBC (Open Database Connectivity) driver instead.

For example, both PowerDesigner™ and NetImpact Dynamo connect through the ODBC driver. Other third-party applications may also require the ODBC driver.

The ODBC connections are built on top of the Open Client Client-Library, so you need to install the Open Client software on the clients where you install the ODBC Driver.

- The Adaptive Server installation program automatically installs the ODBC Driver on the computer on which you install NetImpact Dynamo.
- You can also install the driver separately on other client workstations on which you will be running third-party or developed products.

For more information about the ODBC Driver, see the *ODBC Driver Reference Guide*.

To use ODBC connections, you need to configure the Adaptive Server ODBC driver to allow connection to Adaptive Server.

Configuring the Driver

When you configure the ODBC driver to connect to Adaptive Server, you create an ODBC data source. You can configure more than one data source for Adaptive Server. For example, you might want one data source for each database.

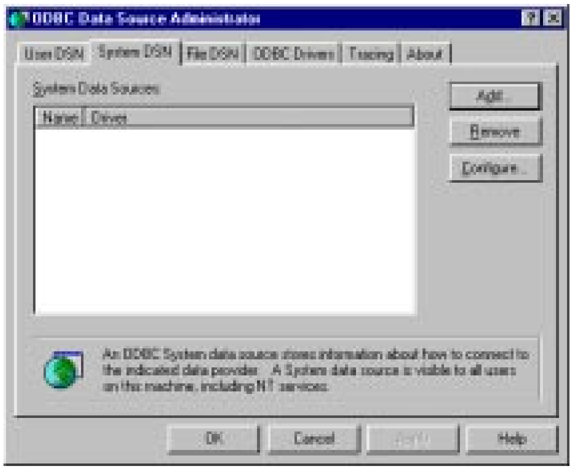
To configure a data source:

1. Start the ODBC Data Source Administrator (*odbcad32.exe*) from the Windows NT System program group.

   For more information about ODBC, see your NT operating system documentation.

2. Click on the System DSN tab to display the System Data Sources dialog box.

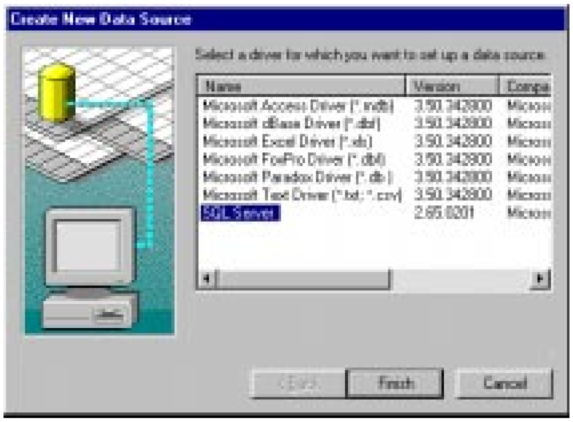
The dialog box appears with a list of sources you might have already defined.



An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users on this machine, including NT services.

3 Click Add to add a new Adaptive Server driver to the list.

The Create New Data Source dialog box appears.

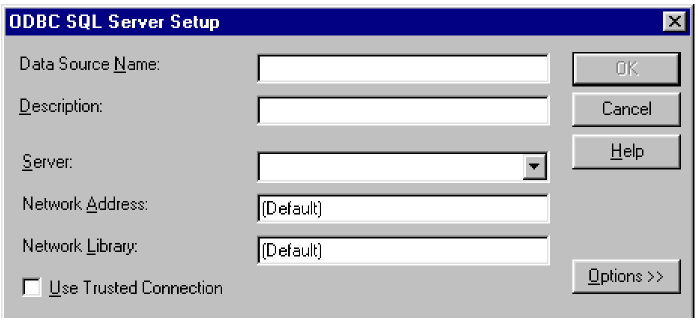


Select a driver for which you want to set up a data source.

Name	Version	Compa
Microsoft Access Driver (*.mdb)	3.50.342800	Micros
Microsoft dBase Driver (*.dbf)	3.50.342800	Micros
Microsoft Excel Driver (*.xls)	3.50.342800	Micros
Microsoft FoxPro Driver (*.dbf)	3.50.342800	Micros
Microsoft Paradox Driver (*.db)	3.50.342800	Micros
Microsoft Text Driver (*.txt; *.csv)	3.50.342800	Micros
SQL Server	2.65.0201	Micros

4 Select SQL Server as the driver you want to use for Adaptive Server, and click Finish.

The ODBC SQL Server Setup dialog box appears.



Network Address: (Default)

Network Library: (Default)

5 Complete the dialog box as follows:

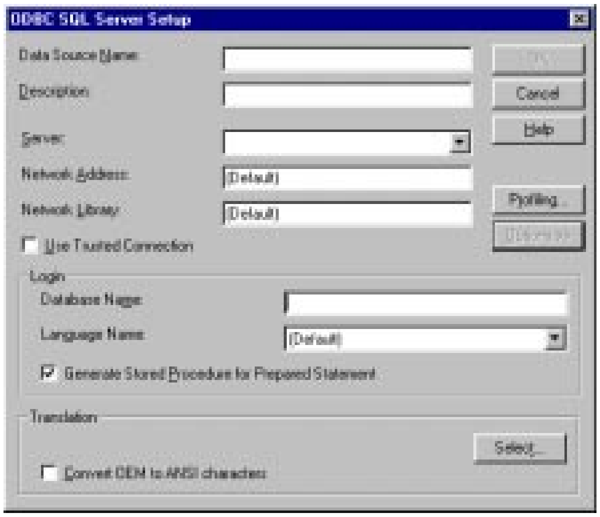
Data Source Name – enter a short description of the Adaptive Server that is meaningful to you. For example, if you are creating the data source to connect to a specific Adaptive Server database, include the database name in the description.

Description (optional) – along description of a data source name; for example, “Accounting database on Adaptive Server 3.”

Server – the name of the Adaptive Server you want to access, as it appears in the *sql.ini* file. If no name is specified, the driver uses the value of the DSQUERY environment variable.

Note Do *not* fill in the Server drop-down list box or the Database Name box for PowerDesigner or NetImpact Dynamo connections.

6 Click the Options button to display the Login box.



ODBC SQL Server Setup

Data Source Name:

Description:

Server:

Network Address: (Default)

Network Library: (Default)

□ Use Trusted Connection

Login

Database Name:

Language Name: (Default)

☑ Generate Stored Procedure for Prepared Statement

Translation

□ Convert OEM to ANSI characters

7 Type the name of the database to which you want to connect in the Database Name text box:

- For a NetImpact Dynamo connection, specify the database. It is a good idea to specify a database for most client connections.
- For a PowerDesigner connection, you do not need to specify a database unless you want to reverse-engineer it. In this case, to "reverse-engineer" means to create a database and then determine its schema, rather than using the normal process of creating the schema first and then creating the database.

You can fill in values for the other parameters in the box. For information about each parameter, see the online help or the *ODBC Driver Reference Guide* in SyBooks.

8 Click OK, and close the rest of the ODBC dialog boxes.

9 Exit the program.

You can now connect to Adaptive Server from applications that require connections through the ODBC Driver. When you start the application and it prompts you for an ODBC data source, choose the data source you have just named and configured.

CHAPTER 4

Tuning Your Operating System to Adaptive Server

This chapter discusses Windows NT operating system issues that you must consider when running Adaptive Server.

Topics covered are:

Adaptive Server Environment Variables

When you install Adaptive Server and other Sybase products on your computer, the installation program adds and modifies several system environment variables in the NT Registry:

- DSLISTEN
- DSQUERY
- PATH
- SYBASE

  When defined with the installation program, the value of SYBASE includes drive information. You can change the drive information, but do not remove the variable.

Note The SYBASE environment variable is not required if the default directory, *\sybase*, is used.

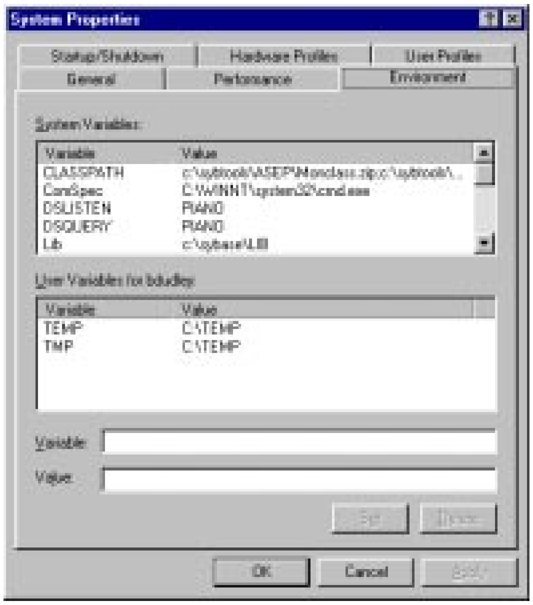
For more information about these variables, see *Adaptive Server Enterprise Installation Guide for Windows NT*.

Displaying the Current Values

You can display the current values for these variables by examining the Environment tab either from:

- The System option in the Windows NT Control Panel, or

- The System Properties dialog box displayed by right-clicking the My Computer icon and selecting Properties from the resulting menu.



System Variables:

Variable	Value
CLASSPATH	c:\sybtools\ASEP\Monclass.zip;c:\sybtools\...
ComSpec	C:\WINNT\system32\cmd.exe
DSLISTEN	PIANO
DSQUERY	PIANO
Lib	c:\sybase\LIB

User Variables for bdudley:

Variable	Value
TEMP	C:\TEMP
TMP	C:\TEMP

Variable:

Value:

The actual Environment NT Registry key stores these values in the following path in the Registry tree:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\Environment
```

For a description of the Adaptive Server Registry keys, see Appendix A, “Adaptive Server Registry Keys”.

Changing Environment Variables

You may want to change the values for the system environment variables when:

- You install multiple versions of Adaptive Server, or
- You intend to access different Adaptive Servers on your network.

Permanent Changes

One method of changing the system environment variables permanently resets their values in the NT Registry. “Permanently” means that the changes continue through server sessions until you manually reset them.

Use the Environment tab in the System option on the Windows NT Control Panel to make such changes.

Temporary Changes

In most cases, you can temporarily change an environment variable by using the **set** command from an NT command prompt. “Temporarily” means that the change lasts only as long as you use the same prompt window, and it remains open.

For example, use the following syntax in a Command Prompt window to temporarily change the value of the DSQUERY system variable for the current window:

```
set DSQUERY = new_value
```

Any Sybase product that you start from the current window uses *new_value* rather than the value specified in the NT Registry. The *new_value* is lost when you close the window or log out of NT.

Note You cannot override the PATH environment variable by using the **set** command.

Other System Adjustments

The Sybase installation program makes several modifications to the variables in the NT Registry. These modifications are in addition to the system environment variables.

These other Registry values control the following aspects of Adaptive Server:

- *Start-up parameters* – See the *Adaptive Server Enterprise Installation Guide for Windows NT*.
- *Error logging* – See “Logging Errors and Events” on page 56.
- *Login security* – See “NT Registry Parameters” on page 107.

Appendix A, “Adaptive Server Registry Keys”, provides a complete list and descriptions of the Adaptive Server Registry values.

Paging File Size

When you install NT, the process creates the paging file at the recommended size, as long as your hard disk has enough space. The recommended size is approximately 1.5 to 2 times the amount of RAM on your system.

Adaptive Server requires that the NT virtual-memory paging file be at or above its recommended size. When the paging file is below the recommended size, Adaptive Server fails to start and gives no indication as to what caused the problem.

For more information about the paging file and how to change its size, see your NT operating system documentation.

CHAPTER 5 Logging Error Messages and Events

This chapter describes how to use the error logging features of Adaptive Server for Windows NT.

Topics covered are:

Logging Errors and Events

Adaptive Server for Windows NT supports two types of message logging:

- Adaptive Server error logging
- Windows NT event logging

Adaptive Server Error Logging

Adaptive Server begins to write information to a local error log file, called the Adaptive Server Error Log each time Adaptive Server starts:

d:\sybase\install\errorlog.log

This error log file:

- Stores information about the success or failure of each start-up attempt.
- Logs error and informational messages generated by the server during its operations.
- Remains open until you stop the server process.
- Retains its contents until you rename, move, or empty the file.

Note When you want to make more memory available by reducing the size of the error log, stop Adaptive Server before deleting logged messages. The log file cannot release its memory space until Adaptive Server has stopped.

Enabling and Disabling Error Logging

Logging to the Adaptive Server Error Log is always enabled. However, when you create or modify a specific user-defined message, you can set it to be omitted from the log. See “Logging User-Defined Messages” on page 67.

Types of Information Logged

The Adaptive Server Error Log stores the following types of messages:

- Start-up messages from Adaptive Server
- Backtraces and stack traces from Adaptive Server
- Fatal error messages (severity level 19 and higher)

- Kernel error messages
- Informational messages

NT Event Logging

Adaptive Server also logs error messages in the NT Event Log, if event logging is enabled.

Using the NT event-logging feature, you can:

- Manage Adaptive Server error messages in the same way that you manage error messages for other NT applications and services
- Set up a central event-logging site to store error messages from multiple Adaptive Servers

For information about centralized event logging, see “Using a Central Logging Site” on page 71.

Setting Up NT Event Logging for Use by Adaptive Server

By default, NT event logging of Adaptive Server messages is enabled, but you can disable it. You can also specify that logging of specific messages always be enabled.

For information about controlling logging of Adaptive Server messages to the NT Event Log, see “Enabling and Disabling NT Event Logging” on page 64.

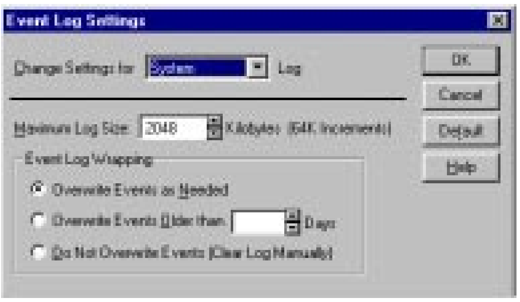
To make NT event logging available to Adaptive Server, ensure that the following conditions are true in the NT Event Log Settings box:

- The Overwrite Events as Needed option is selected
- The Maximum Log Size is set to at least 2048 bytes

Use the NT Event Viewer to confirm or change these settings:

1. Choose Programs from the Start menu, choose Administrative Tools (Common), and choose Event Viewer.
2. Choose Log Settings from the Log menu.

The Event Log Settings dialog box appears. Make sure that the System Log is selected.



Change Settings for System Log

Maximum Log Size: 2048 Kilobytes (64K Increments)

Event Log Wrapping

● Overwrite Events as Needed

○ Overwrite Events Older than Days

○ Do Not Overwrite Events (Clear Log Manually)

3 Change the Maximum Log Size to 2048, if necessary.

4 Click the Overwrite Events as Needed button to toggle the feature on or off.

5 Click OK.

6 Choose Exit from the Log menu.

Types of Information Logged

Adaptive Server for NT logs the same messages in the NT Event Log as in its Adaptive Server Error Log, with the exception of normal start-up messages. Some start-up messages are recorded only in the NT Event Log, but all messages are logged in the local Adaptive Server Error Log.

Optionally, you can specify the recording of successful and unsuccessful logins to Adaptive Server in the Adaptive Server Error Log and the NT Event Log. See “Logging User-Defined Messages” on page 67.

Managing the Logs

Table 5-1 names the parameters, options, and system procedures for enabling and disabling event and error logging and indicates whether they affect the two logs. It also lists the pages in this chapter that contain instructions on using these elements to refine message logging.

Table 5-1: Methods for enabling/disabling error and event logging

Method	Affects Event Log	Affects Error Log	See
error logging configuration parameter	Yes	No	65
event log computer name configuration parameter	Yes	No	65, 70
Server Config Event Logging option	Yes	No	65
Server Config Error Log Path option	No	Yes	60, 76
sp_altermessage system procedure	Yes	Yes	67
sp_addmessage system procedure	Yes	Yes	67
log audit logon success configuration parameter	Yes	Yes	68
log audit logon failure configuration parameter	Yes	Yes	68
xp_logevent system extended stored procedure	Yes	No	68

Setting Error Log Paths

The installation program sets the error log location in the Sybase installation directory when you configure a new Adaptive Server. Backup Server and Monitor Server each have their own error logs.

The default location for each server's error log is:

- Adaptive Server: *\install\errorlog*
- Backup Server: *\install\backup.log*
- Monitor Server: *\install\ms.log*

At start-up, you can reset the name and location of the Adaptive Server Error Log file from the command line. Use the **-e** start-up parameter and value in the **isql** command to start Adaptive Server.

To change the default error log path or file name:

- For Adaptive Server, see "Setting the Adaptive Server Error Log Path" on page 60
- For Backup Server, see "Setting the Backup Server Error Log Path" on page 61
- For Monitor Server, see "Setting the Monitor Server Error Log Path" on page 62

Note Multiple Adaptive Servers cannot share the same error log. If you install multiple Adaptive Servers, be sure to specify a unique error log file name for each server.

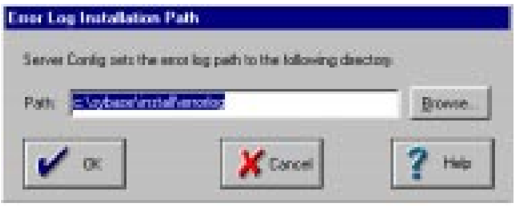
Setting the Adaptive Server Error Log Path

Use the Server Config utility to change the path:

1. Choose Programs from the Start menu, choose Sybase, and choose Server Config.
2. Click the Adaptive Server icon from the Products box in the Configure Sybase Servers dialog box.
3. Click the Configure Adaptive Server button in the Adaptive Server Enterprise box.

4. Select the name of the server to configure in the Existing Servers box, and click Continue.
5. Type the login name and password of an Adaptive Server user with System Administrator privileges in the Enter System Administrator Password dialog box.
6. Click Continue.
7. Click Yes if Adaptive Server is not running, and Server Config prompts you to start it.
8. Click the Error Log Path button in the Configure Adaptive Server Enterprise dialog box.

   Server Config displays the Error Log Installation Path dialog box:



Error Log Installation Path

Server Config sets the error log path to the following directory:

Path: c:\sybase\install\errorlog

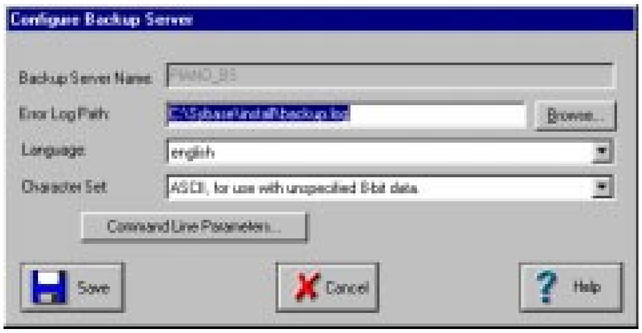
9. Type the full path name to an error log file that is not on a network drive, and click OK.
10. In the Configure Adaptive Server dialog box, click the Save button to save the new error log setting.
11. Click Exit to quit Server Config.

Setting the Backup Server Error Log Path

Use the Server Config utility to change the path:

1. Choose Programs from the Start menu, choose Sybase, and choose Server Config.
2. Click the Backup Server icon from the Products box in the Configure Sybase Servers dialog box.
3. Click the Configure Backup Serve button in the Backup Server box.
4. Select the name of the server to configure in the Existing Servers box, and click Continue.

5 Type the full path name to an error log file that is not on a network drive in the Configure Backup Server dialog box.



Backup Server Name: PIANO_BS

Error Log Path: C:\Sybase\install\backup.log

Language: english

Character Set: ASCII, for use with unspecified 8-bit data

6 Click the Save button to save the new error log setting.

7 Click Exit to quit Server Config.

Setting the Monitor Server Error Log Path

Use the Server Config utility to change the path:

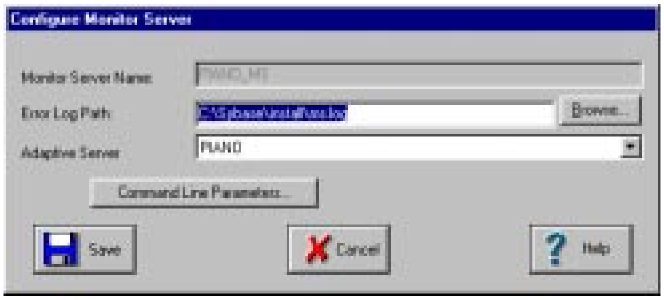
1 Choose Programs from the Start menu, choose Sybase, and choose Server Config.

2 Click the Monitor Server icon from the Products box in the Configure Sybase Servers dialog box.

3 Click the Configure Monitor Server button in the Monitor Server box.

4 Select the name of the server to configure in the Existing Servers box, and click Continue.

5 Type the full path name to an error log file that is not on a network drive in the Configure Monitor Server dialog box.



Configure Monitor Server

Monitor Server Name: PIANO_MS

Error Log Path: C:\Sybase\install\ms.log

Adaptive Server: PIANO

6 Click the Save button to save the new error log setting.

7 Click Exit to quit Server Config.

Enabling and Disabling NT Event Logging

By default, Adaptive Server enables the logging of its messages to the NT Event Log at start-up. This section explains how to disable and enable logging of Adaptive Server messages to the NT Event Log.

There are two ways to control event logging:

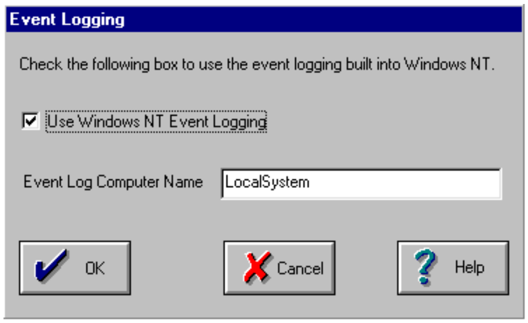
- Using Server Config
- Using sp_configure

Using Server Config

Use the Server Config utility to control event logging:

1. Choose Programs from the Start menu, choose Sybase, and Choose Server Config.
2. Click the Adaptive Server icon, and click the Configure Adaptive Server button.
3. Select the name of the server to configure in the Existing Servers dialog box, and click Continue.
4. Type the login name and password of an Adaptive Server user with System Administrator privileges in the Enter System Administrator Password dialog box.
5. Click Continue.
6. Click Yes if the Adaptive Server is not running, and Server Config asks you to start it now.
7. Click Event Logging in the Configure Adaptive Server Enterprise dialog box.

Server Config displays the Event Logging dialog box:



Event Logging

Check the following box to use the event logging built into Windows NT.

☑ Use Windows NT Event Logging

Event Log Computer Name: LocalSystem

8. Click the Use Windows NT Event Logging button to enable or disable Adaptive Server error message logging to the NT Event Log.
9. In the Event Log Computer Name text box:
    - To send messages to a remote computer log, type its name.
    - To send messages to a local computer log, let the value default to LocalSystem.
10. Click OK.
11. Click Save to save your changes in the Configure Adaptive Server dialog box.
12. Click Exit to quit Server Config.

Using *sp_configure*

You can enable Adaptive Server message storage in the NT Event Log by using the **sp_configure** system procedure to set the **event logging** configuration parameter. Possible values are:

- 1 – to enable logging of Adaptive Server messages

  ```
  sp_configure "event logging", 1
  ```

- 0 – to disable logging of Adaptive Server messages

```
sp_configure "event logging", 0
```

Note Restart Adaptive Server after enabling logging with **sp_configure**; disabling does not require a server restart.

For information about the **event logging** configuration parameter and **sp_configure** in general, see the *System Administration Guide*.

Managing Messages

When event logging is enabled, you can manage its functions in the following ways:

- Use the **sp_addmessage** or **sp_altermessage** system procedure to control whether a specific user-defined message is logged in both the Adaptive Server Error Log and in the NT Event Log.

  For the complete syntax for the **sp_addmessage** and **sp_altermessage** system procedures, see the *Adaptive Server Reference Manual*.

- Use configuration parameters to specify whether auditing events are logged. Auditing events pertain to a user's success, **log audit logon success**, or failure, **log audit logon failure**, in logging into Adaptive Server.
- Use the **xp_logevent** extended stored procedure to set up logging of user-defined events in the NT Event Log in Adaptive Server.

Logging User-Defined Messages

You can specify whether a user-defined message is logged to the Adaptive Server Error Log as well as to the Windows NT Event Log. Adaptive Server lets you make this determination for:

- New messages (**sp_addmessage**)
- Existing messages (**sp_altermessage**)

For more information about these commands and their parameters, see **sp_addmessage** and **sp_altermessage** in the *Adaptive Server Reference Manual*.

New Messages

Include the **with_log** option in the **sp_addmessage** system procedure when you add a new user-defined message to *sysusermessages*. This parameter sets the Adaptive Server to log the message each time that the message appears.

Existing Messages

Include the **with_log** option in the **sp_altermessage** system procedure to change an existing user-defined message. This parameter alters the reporting status of that message:

- TRUE – to enable logging
- FALSE – to disable logging

Logging Auditing Events

By default, Adaptive Server does not log auditing events. However, you can use **sp_configure** parameters to specify whether Adaptive Server is to log auditing events, such as logins, to the Adaptive Server Error Log and to the NT Event Log.

Possible parameters and values are:

- **log audit logon success** at 1 – to enable logging of successful Adaptive Server logins

  ```
  sp_configure "log audit logon success", 1
  ```

- **log audit logon failure** at 1 – to enable logging of unsuccessful Adaptive Server logins

  ```
  sp_configure "log audit logon failure", 1
  ```

- Either parameter at 0 – to disable logging of that message type.

  ```
  sp_configure "log audit logon success", 0
  sp_configure "log audit logon failure", 0
  ```

For more information about the **sp_configure** system procedure, see the *System Administration Guide*.

Logging User-Defined Events

You can arrange to have user-defined events logged to the NT Event Log from within Adaptive Server. For example, you can create a “database imported” event that is generated after a database has been imported successfully.

Using the **xp_logevent** extended stored procedure (ESP), you can arrange to log the event. This ESP allows you to specify the following:

- The message that is to appear in the event description field of the event viewer when the event is logged
- Whether the event should be characterized as informational, warning, or error

For more information, see **xp_logevent** in the *Adaptive Server Reference Manual*.

Using a Remote Log

By default, if event logging is enabled, Adaptive Server logs messages to the NT Event Log on the local computer system.

To change the destination computer for logging messages:

1 Set the **event log computer name** configuration parameter with **sp_configure** on the local computer. Use either:

- The **sp_configure** system procedure, as in the following command line, or

  ```
  sp_configure "event log computer name", 0, user1
  ```

- Enter the name of the target computer in the Event Log Computer Name box on the Event Logging dialog box.

  To display the name box, see "Using Server Config" on page 64.

2 Start the server from a Domain Administrators account.

  a Choose Settings from the Start menu, choose Control Panel, and choose Services.

  b Select the remote server to use from the list.

  c Click the Startup button.

  d Click This Account in the Log On As box.

  e Open the drop-down list to display the Add Users dialog box.

  f Double-click an account name that is in the Domain Administrators group, and click OK.

  g Click OK at the Service dialog box.

  h Click Start to exit the utility and enable the server.

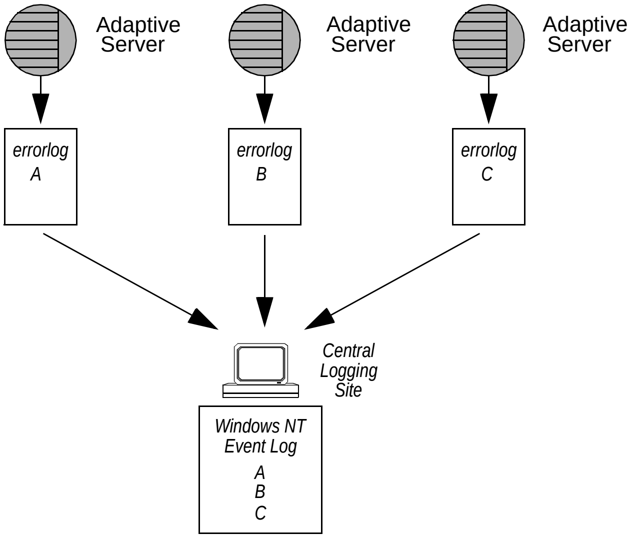
Regardless of how you specify the destination computer, be sure that it is configured to record Adaptive Server error messages. To configure the destination computer, see "Using a Central Logging Site" on page 71.

Using a Central Logging Site

You can record messages from multiple Adaptive Servers in the NT Event Log of a central, network computer. The recording computer does not need to run Adaptive Server.

Figure 5-1 illustrates a central logging site.

Figure 5-1: Diagram of a central logging site



Using a central logging site provides added flexibility in managing multiple Adaptive Servers. For example:

- A System Administrator can monitor the status of all Adaptive Servers on the network by examining the central event log.
- Users of individual Adaptive Servers can view either the local Adaptive Server Error Log file or the central event logging site to examine error messages.

Logging Messages from Multiple Adaptive Servers

To log messages from multiple Adaptive Servers, the central logging computer must have:

- Access to the *sybevent.dll* file

- A Registry key for each Adaptive Server that will log messages on the central computer
- A set of four key values that define each Registry key for Adaptive Server

Setting Up a Local Central Logging Site

An event-logging computer uses a Registry key to define each message-sending Adaptive Server and is unable to log messages from servers for which it has no key.

To set up a computer as a central logging site, you must create and define a Registry key for each Adaptive Server that is to log messages into the site.

To Create and Define a Registry Key

Use the *sybevent.dll* file and the **regedt32** utility.

To create and define a Registry key:

1. Log into Windows NT using an account with NT administrator privileges.
2. Copy the *sybevent.dll* file from an Adaptive Server machine if it does not exist on the local computer.

   The *sybevent.dll* file is stored in the *dll* subdirectory of the Sybase installation directory (*\sybase\dll*, by default). The actual location of *sybevent.dll* on the logging computer is not important, however, you must record a fixed location for the file in the NT Registry.

   Note You can use the same *sybevent.dll* file on the event-logging computer, as long as all Adaptive Servers are at the same Version level; for example, 11.5.1.

3. Start the NT **regedt32** utility.

   For instructions and screens on using this utility with Adaptive Server, see “Increasing Windows Sockets Connections” on page 32.

4. Complete the steps in “Creating a Registry key” on page 73 to create a key for a single Adaptive Server.
5. Complete the steps in “Defining a Registry key” on page 73 to define the key that you just created.

6 Repeat steps 4 and 5 for each Adaptive Server that is to send messages to the logging site computer.

Creating a Registry key

To create a Registry Key:

1 In the **regedt32** utility, select the Registry window named HKEY_LOCAL_MACHINE.

2 Open the levels until you reach the Registry key named:

HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\EventLog\Application

3 From the Edit menu, choose Add Key to display the Add Key dialog box:

4 Complete the dialog box as follows:

Key Name – Type the name of the Adaptive Server computer that is to store the messages at the central logging site.

Class – Leave this box blank. You do not have to specify a class for the new key.

5 Verify that you have entered the new Registry key correctly.

6 Click OK.

7 Complete the steps in “To define a Registry key:” on page 73 to define the key that you just created.

Defining a Registry key

To define a Registry key:

1 In the **regedt32** utility, open the Registry key that you just created.

2 From the Edit menu, choose Add Value.

3 Type an event-logging value name as shown in Table 5-2 for the new Registry key.

Enter the value name exactly as it is shown in the table; value names are case sensitive.

Table 5-2: Registry values for a central logging PC

Value Name	Datatype	String	Notes
CategoryCount	REG_DWORD	0x6	Do not change the data value. Make sure the string value is hexadecimal (Hex).
CategoryMessageFile	REG_SZ	*D:\SYBASE\DLL\ SYBEVENT.DLL*	Replace *d:\sybase\dll* with the path to the *sybevent.dll* file.
EventMessageFile	REG_SZ	*D:\SYBASE\DLL\ SYBEVENT.DLL*	Replace *d:\sybase\dll* with the path to the *sybevent.dll* file.
TypesSupported	REG_DWORD	0xff	Do not change the data value. Make sure the string value is hexadecimal (Hex).

Note Be sure to enter the correct path to the *sybevent.dll* file for the CategoryMessageFile and EventMessageFile values.

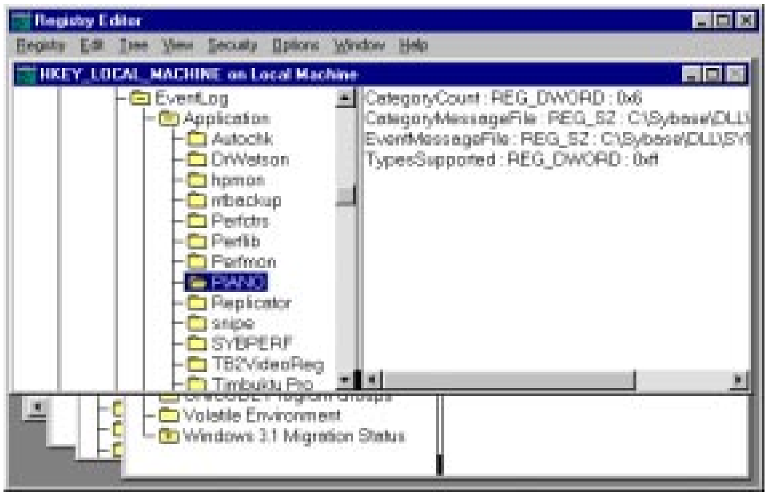
4 Select the data type for the value as named in Table 5-2 from the drop-down list.

5 Verify that you have entered the new key value and data type correctly, and click OK.

6 Type the data or string in the Editor box, and click OK.

7 Repeat steps 2–6 for the remaining three values in each Registry Key.

The following screen shows a sample Registry Key with the four values for the server named PIANO.



CategoryCount : REG_DWORD : 0x6
CategoryMessageFile : REG_SZ : C:\Sybase\DLL\
EventMessageFile : REG_SZ : C:\Sybase\DLL\SY
TypesSupported : REG_DWORD : 0xff

8 To create another key begin again with “To create a Registry Key:” on page 73.

9 Once you have created a Registry key for each Adaptive Server, choose Exit from the Registry menu in the Registry Editor dialog box to quit **regedt32**.

Viewing the Messages

You need the NT Event Viewer and a text editor to display the error messages and events that have been logged.

In the NT Event Log

Use the NT Event Viewer in the Administrative Tools group.

To examine Adaptive Server messages recorded in the NT Event Log:

1. Choose Programs from the Start menu, choose Administrative Tools (Common), and choose Event Viewer.

   The Viewer displays a list of Adaptive Server messages.

2. Double-click on a message to display its Event Detail dialog box.

   The Description list box defines the Adaptive Server message number as a number and text.

In the Adaptive Server Error Log

Use a text editor, such as NotePad, on the logging computer to open the file and view the messages in the Adaptive Server Error Log.

If you are cannot find the error log file:

1. Choose Programs from the Start menu, choose Sybase, and choose Server Config.
2. Click the Adaptive Server icon, and click the Configure Adaptive Server button.
3. Select the name of the server whose error log you want to examine from the Existing Servers dialog box, and click Continue.
4. Type the login name and password of an Adaptive Server user with System Administrator privileges in the Enter System Administrator Password dialog box.
5. Click Continue.
6. Click Yes if the Adaptive Server is not running, and Server Config asks you to start it now.

7 Click Error Log Path from the Configure Adaptive Server dialog box.

Server Config displays the Error Log Installation Path dialog box, which supplies the current path to the Error Log.

For detailed information on interpreting the information in the Error Log, see the *System Administration Guide*.

CHAPTER 6

Using Security Services with NT LAN Manager

This chapter describes how to use Adaptive Server security services with the Windows NT LAN Manager to authenticate users and provide data integrity.

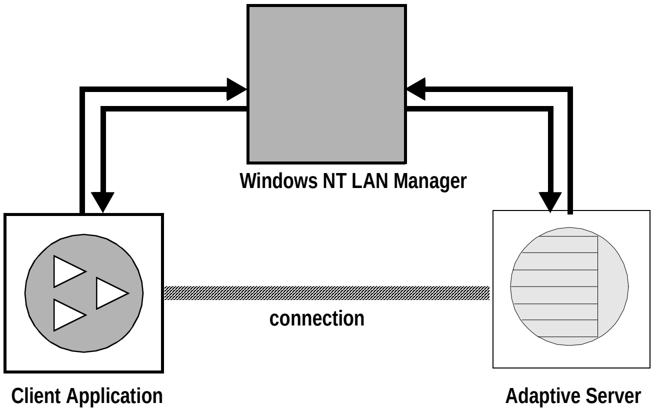
Topics covered are:

Security Services with NT LAN Manager

When using Adaptive Server on NT, you can enable the security services provided by NT LAN Manager to authenticate users, clients, and servers to one another.

Figure 6-1 shows a client application that is using LAN Manager to ensure a secure connection with Adaptive Server.

Figure 6-1: Establishing secure connections between LAN Manager and Adaptive Server



The secure connection between LAN Manager and a server can be used to provide a unified login to Adaptive Server. Through this login, the LAN Manager authenticates users *once* and does not require them to supply a name and password every time they log into Adaptive Server.

The secure connection also can support one or more of the following security services:

- Message integrity to verify that data communications have not been modified
- Replay detection to verify that data has not been intercepted by an intruder
- Out-of-sequence check to verify the order of data communications

How Login Authentication Works

When a client requests authentication services, the following steps occur:

1. The client validates the login with LAN Manager. LAN Manager returns a *credential*, which contains security-relevant information.
2. The client sends the credential to Adaptive Server and informs Adaptive Server that it wants to establish a secure connection.
3. Adaptive Server authenticates the client’s credential with LAN Manager.

   When the credential is valid, Adaptive Server establishes a secure connection between itself and the client.

Administering Security Services Using LAN Manager

Table 6-1 describes a process for using Adaptive Server's unified login capability with LAN Manager.

Warning! Adaptive Server must be installed before completing the steps in Table 6-1.

Table 6-1: Process for administering network-based security

Step	Description	See
1. Set up the configuration files: - *libtcl.cfg* - *sql.ini*	Use a text editor to modify the *libtcl.cfg* file. Use dsedit to specify security mechanisms in the *sql.ini* file or a Directory Service.	"Modifying Configuration Files for a Unified Login" on page 84 *Open Client/Server Configuration Guide for Desktop Platforms*
2. Make sure the security administrator for LAN Manager has created logins for each user and for the Adaptive Server and Backup Server.	The security administrator for LAN Manager must add names and passwords for users and servers.	"Identifying Users and Servers to LAN Manager" on page 88 NT LAN Manager documentation
3. Configure security for the installation.	Use sp_configure to enable the use of security services.	"Configuring Adaptive Server for LAN Manager Security" on page 89
4. Restart Adaptive Server.	Activates the use security services parameter.	"Initiating the New Security Services" on page 94
5. Add logins to Adaptive Server to support enterprise-wide login.	Use sp_addlogin to add users. Optionally, specify a default secure login with sp_configure.	"Adding Logins to Support Unified Login" on page 95

Step	Description	See
6. Connect to the server.	Use isql with the -V option or use Open Client Client-Library to connect to Adaptive Server and specify the security services to use. Note: if you use the isql utility, you do not have to supply a username or password.	"Defining the Connection to a Server for Security Services" on page 97 *Open Client/Server Configuration Guide for Desktop Platforms* "Security Features" topics page in the *Open Client Client-Library Reference Manual*

Modifying Configuration Files for a Unified Login

Configuration files are created during installation at a default location in the Sybase directory structure. Table 6-2 provides an overview of the configuration files required for LAN Manager to use unified login and security services.

Table 6-2: Names and locations for configuration files

File Name	Description	Directory
libtcl.cfg	This driver configuration file contains information pertaining to directory, security, and network drivers and any required initialization information.	*d:\sybase\ini*
objectid.dat	This object identifiers file maps global object identifiers, such as the LAN Manager, to local names for character set, collating sequence, and security mechanisms.	*d:\sybase\ini*
sql.ini	The *sql.ini* file contains connection and security information for each server that it lists.	*d:\sybase\ini*

For a detailed description of the configuration files, see the *Open Client/Server Configuration Guide for Desktop Platforms*.

Setting Up Drivers for Network-Based Security

The *libtcl.cfg* file stores information about the following driver types:

- Network (Net-Library)
- Directory Services
- Security

A **driver** is a Sybase library that provides an interface to an external service provider. Adaptive Server dynamically loads drivers so you can change the driver used by an application without relinking the application.

Entries for Network Drivers

The syntax for a network driver entry in the *libtcl.cfg* file is:

```
driver=protocol description
```

where:

- *driver* is the name of the network driver.
- *protocol* is the name of the network protocol.

- *description* is a description of the entry.
  This element is optional.

Note You can comment out the network driver entry by placing a semicolon at the beginning of the line. Then, Adaptive Server uses a driver that is compatible with your application and platform.

Entries for Directory Services

Entries for Directory Services apply if you want to use a Directory Service instead of the *sql.ini* file.

For information about directory entries, see "Sharing Network Configuration Information" on page 39.

Warning! Client applications bundled with Adaptive Server require an *sql.ini* file for effective processing. Eliminating this file with a directory service might be efficient, but it also might limit Adaptive Server functionality.

Entries for Security Drivers

The syntax for a security driver entry in the *libtcl.cfg* file is:

```
provider=driver
```

where:

- *provider* is the local name for the security mechanism. *objectid.dat* defines the mapping of the local name to a global object identifier. The default local name for NT LAN Manager on Windows NT and Windows 95 (for clients only) is "LIBSMSSP".

  Note If you use a provider name other than the default, you must also change the local name in the *objectid.dat* file. For an example, see "Checking the LAN Manager's Local Name" on page 86.

- *driver* is the name of the security driver. The NT LAN Manager driver is named "LIBSMSSP." The default location of all drivers is *d:\sybase\dll*.

Editing the *libtcl.cfg* File

Use the **ocscfg** utility to edit the *libtcl.cfg* file. This utility displays the file's contents in a dialog box with section headings in the form of tabs for easy perusal.

For information on using the **ocscfg** utility, see the *Open Client/Server Configuration Guide for Desktop Platforms*.

The following text is a sample *libtcl.cfg* file for desktop platforms:

```
[NT_DIRECTORY]
 ntreg_dsa=LIBDREG  ditbase=software\sybase\serverdsa
[DRIVERS]
 NLWNSCK=TCP  Winsock TCP/IP Net-Lib driver
 NLMSNMP=NAMEPIPE  Named Pipe Net-Lib driver
 NLNWLINK=SPX  NT NWLINK SPX/IPX Net-Lib driver
 NLDECNET=DECNET  DecNET Net-Lib driver
[SECURITY]
 NTLM=LIBSMSSP
```

Checking the LAN Manager's Local Name

The *objectid.dat* file maps global object identifiers to local names.

Note You need to change this file only if you have changed the local name of the LAN Manager in the *libtcl.cfg* file.

The file contains sections such as [CHARSET] for character sets and [SECMECH] for security services. Of interest here is the security section.

The following example is a security section excerpt from the *objectid.dat* file:

```
[secmech]
      1.3.6.1.4.1.897.4.6.3   = NTLM
```

You can specify only one local name for LAN Manager. Use any text editor to edit this file.

Warning! Do not change the "1.3.6.1.4.1.897.4.6.3" identification.

Specifying Security Information for Adaptive Server

You can use the *sql.ini* file or a Directory Service to provide information about the servers in your installation.

To use either the *sql.ini* file or a Directory Service, run the **dsedit** utility. This utility provides a graphical user interface for specifying server attributes such as the server version, name, and security mechanism.

For information about using **dsedit**, see the *Open Client/Server Configuration Guide for Desktop Platforms*.

For more information about using directory services with Adaptive Server on Windows NT, see “Sharing Network Configuration Information” on page 39.

Identifying Users and Servers to LAN Manager

The security administrator for LAN Manager must define *principals* (defined users) to the security mechanism. Use LAN Manager's User Manager utility to identify all users for the system.

You do not need to enter the Adaptive Server name as a principal to LAN Manager. However, the NT user account that you use to start Adaptive Server must be defined as a valid principal to LAN Manager. For example, to use an NT account named "servadmin" to start Adaptive Server, you must define "servadmin" as a principal to LAN Manager.

This rule applies whether you start Adaptive Server through Sybase Central or as an NT service. See *Adaptive Server Enterprise Installation Guide for Windows NT*.

For detailed information about the User Manager utility, see your NT LAN Manager documentation.

Configuring Adaptive Server for LAN Manager Security

Adaptive Server uses several configuration parameters to administer unified login and security services through LAN Manager. To set these parameters, you must be a System Security Officer.

All parameters for unified login and security through LAN Manager are part of the “Security-Related” configuration parameter group. Use the configuration parameters to:

- Enable the use of external security services (LAN Manager)
- Require unified login
- Require one or more message integrity security services

Enabling and Disabling External Security Services

To reset the status of LAN Manager security services, use **sp_configure** with the **use security services** configuration parameter:

- 1 – to enable services with LAN Manager
- 0 – the default, to disable network-based security services

The syntax is:

```
sp_configure "use security services", [0|1]
```

For example, to enable services with LAN Manager, execute:

```
sp_configure "use security services", 1
```

Managing Unified Login

You can use configuration parameters to:

- Require unified login
- Establish a default secure login

Because all the parameters for unified login are dynamic, they take effect as soon as you change them. You must be a System Security Officer to set the parameters.

Requiring Unified Login

The **unified login required** configuration parameter controls the type of login that is acceptable to Adaptive Server. The possible values are:

- 1 – to require all users who request a connection to Adaptive Server to be authenticated by LAN Manager
- 0 – the default, to let Adaptive Server accept both traditional login names and passwords and authenticated credentials

The syntax is:

```
sp_configure "unified login required", [0|1]
```

For example, to require all logins to be authenticated by a security mechanism, execute:

```
sp_configure "unified login required", 1
```

Establishing a Secure Default Login

When a user with a valid credential from LAN Manager logs into Adaptive Server, the server checks to see whether the name is listed as a user in *master..syslogins*. If it is, Adaptive Server accepts that user name.

For example, a user logs into LAN Manager as “ralph”, and “ralph” is listed in *master..syslogins*. Adaptive Server uses all roles and authorizations as defined for “ralph” on that server.

As an alternative example, a user with a valid credential logs into Adaptive Server, but is unknown to the server. Adaptive Server accepts the login only when a *secure default login* has been defined with **sp_configure**. Adaptive Server uses the default login for any user who is not defined in *master.syslogins*, but who is validated by LAN Manager.

To set up a secure login, use the following syntax:

```
sp_configure "secure default login", 0, login_name
```

where *login_name* is a user name. The default value for the **secure default login** parameter is “guest”.

The login used for this parameter must be a valid login in *master..syslogins*. For example, to set the login “gen_auth” to be the default login.

1. Use **sp_addlogin** to add the login as a valid user in Adaptive Server:

   ```
   sp_addlogin gen_auth, pwgenau
   ```

   This procedure sets the initial password to “pwgenau”.

2. Use **sp_configure** to designate the login as the security default:

   ```
   sp_configure "secure default login", 0, gen_auth
   ```

   Adaptive Server then uses this login for a user who, although validated by LAN Manager, is unknown to Adaptive Server.

Note Be aware that this user does not have a unique identity in Adaptive Server. That is, more than one user can assume the *suid* (system user ID) associated with the secure default login. You might want to activate auditing for all activities of the default login. Instead of using the secure default login, consider using **sp_addlogin** to add all users to the server.

For more information about adding logins, see “Adding Logins to Support Unified Login” on page 95.

Mapping LAN Manager Login Names to Server Names

All login names in Adaptive Server must be valid identifiers. However, external security mechanisms, such as LAN Manager, may allow login names that are not valid in Adaptive Server.

For example, login names that are longer than 30 characters or that contain special characters such as !, %, *, and & are invalid names in Adaptive Server.

Table 6-3 shows how Adaptive Server converts invalid characters in login names:

Table 6-3: Conversion of invalid characters in login names

Invalid Character	Converts To
Ampersand &	Underscore _
Apostrophe ’	
Backslash \	
Colon :	
Comma ,	
Equals sign =	
Left single quotation mark ‘	
Percent sign%	
Right angle bracket >	
Right single quotation mark ’	
Tilde ~	

Invalid Character	Converts To
Caret ^ Curly brackets { } Exclamation point ! Left angle bracket < Parentheses ( ) Period . Question mark ?	Dollar sign $
Asterisk * Minus sign - Pipe | Plus sign + Quotation marks " Semicolon ; Slash / Square brackets [ ]	Pound sign #

For more information about identifiers, see the *System Administration Guide*.

Requiring Data Integrity Check

You can use the following configuration parameters with LAN Manager. These parameters cause Adaptive Server to check one or more types of data integrity for all messages.

- **msg integrity reqd** – set this parameter to 1 to force a check for general tampering in all messages.

  If the parameter is set to 0 (the default), message integrity is not required. However, the client can establish this check if the security mechanism supports it.

- **msg out-of-seq checks reqd** – set this parameter to 1 to force a check for sequence changes in all messages.

  If the parameter is set to 0 (the default), sequence checking is not required. However, the client can establish this check if the security mechanism supports it.

- **msg replay detection reqd** – set this parameter to 1 to force a check for replay or interception in all messages.

  If the parameter is set to 0 (the default), replay detection is not required. However, the client can establish this check if the security mechanism supports it.

Ensuring Adequate Memory for Security Services

The value of the **total memory** configuration parameter specifies the number of 2K blocks of memory that Adaptive Server requires at start-up. To make sure that there is sufficient memory when using unified login and security services through LAN Manager, be sure to allocate approximately 6K of additional memory per connection.

For example, if the maximum number of unified logins that occur at the same time is expected to be 150, increase the **total memory** parameter by 450. This increase expands memory allocation by 450 2K blocks.

The syntax is:

```
sp_configure total memory, value
```

where *value* is the sum of the current memory and the memory you are adding.

For example, to supply Adaptive Server with 25,000 2K blocks of memory, including the increased memory for network-based security, enter:

```
sp_configure total memory, 25000
```

The minimum requirement for this parameter is specific to the operating system. For more information, see your Windows NT operating system documentation.

For information about estimating and specifying memory requirements for Adaptive Server, see the *System Administration Guide*.

Initiating the New Security Services

Changes to the security services are static. You must restart Adaptive Server to activate the security services.

For instructions on starting and stopping Adaptive Server, see *Adaptive Server Enterprise Installation Guide for Windows NT*.

Adding Logins to Support Unified Login

When a user logs into Adaptive Server with an authenticated credential, Adaptive Server follows these steps, as needed:

1. Checks that user is a valid user in *master..syslogins*.
    - If the username appears, Adaptive Server accepts the login without requiring a password.
    - If the user name does not appear, Adaptive Server performs step 2.
2. Checks that a default secure login is defined in *master..syslogins*.
    - A default login definition allows the user to log in successfully.
    - The absence of a default login definition causes Adaptive Server to reject the login.

Therefore, consider whether to allow only users who are defined as valid logins to use Adaptive Server or to allow any user with the default login to use Adaptive Server.

Note You must add the default login in *master..syslogins* and use **sp_configure** to define the default. For more information, see "Establishing a Secure Default Login" on page 90.

General Procedure for Adding Logins

To add logins to the server and, optionally, to add users with appropriate roles and authorization to one or more databases, follow the general procedure described in Table 6-4.

Table 6-4: Adding logins and authorizing database access

Task	Required Role	Command or Procedure	See
1. Add a login for the user.	System Security Officer	sp_addlogin	The *System Administration Guide*
2. Add the user to one or more databases.	System Security Officer, System Administrator, or Database Owner	sp_adduser Enter this procedure from within the database.	The *System Administration Guide*

Task	**Required Role**	**Command or Procedure**	**See**
3. Add the user to a group in a database.	System Security Officer, System Administrator, or Database Owner	sp_changegroup Enter this procedure from within the database.	The *System Administration Guide* sp_changegroup in the *Adaptive Server Reference Manual*
4. Grant system roles to the user.	System Administrator or System Security Officer	grant role	The *System Administration Guide* grant in the *Adaptive Server Reference Manual*
5. Create user-defined roles and grant the roles to users.	System Security Officer	create role grant role	The *System Administration Guide* grant role in the *Adaptive Server Reference Manual* create role in the *Adaptive Server Reference Manual*
6. Grant access to database objects.	Database object owner	grant [select | insert| delete| update| references | execute]	The *System Administration Guide*

Defining the Connection to a Server for Security Services

Use the following options to define an Adaptive Server for network-based security services such as NT LAN Manager through the **isql** and **bcp** utilities:

- **-R** *remote_server_principal* – to specify the principal name for Adaptive Server
- **-V** *security_options* – to specify network-based user authentication
- **-Z** *security_mechanism* – to specify the name assigned to LAN Manager

For more information about Adaptive Server utilities, see *Utility Programs for Windows 95, Windows 98, and Windows NT*.

Specifying the Principal Name

Use **-R** *remote_server_principal* to specify the principal name for the server as defined for LAN Manager.

By default, a server's principal name matches the server's network name, which is specified by either the **-S** option or the DSQUERY environment variable. You must use the **-R** option when the server's principal name and network name are not the same.

Specifying Network-Based User Authentication

Use **-V** *security_options* to specify network-based user authentication.

With this option, the user must log into NT LAN Manager before running the utility. In this case, if a user specifies the **-U** option, the user must supply the network user name known to the security mechanism, and any password supplied with the **-P** option is ignored.

-V can be followed by a *security_options* string of key-letter options to enable additional security services. The key letters are:

- **i** – to enable data integrity service. This option verifies that data communications have not been modified.
- **r** – to enable data replay detection. This option verifies that data has not been intercepted by an intruder.

- **q** – to enable out-of-sequence detection. This option verifies the order of data communications.

You can specify additional security options by including them immediately following the **-V** option. For example, to use **isql** with network-based user authentication, replay detection, and out-of-sequence detection, enter:

```
isql -Vrq
```

Specifying the Name Assigned to LAN Manager

The **-Z** *security_mechanism* specifies the name assigned to LAN Manager in the *libtcl.cfg* configuration file; “LIBSMSSP”, by default.

When the line does not supply a *security_mechanism* name, the command uses the default mechanism.

For more information about security mechanism names, see the *Open Client/Server Configuration Guide for Desktop Platforms*.

Note When you log into LAN Manager and then log into Adaptive Server, you do not need to specify the **-U** (user) option on the utility because Adaptive Server gets the username from LAN Manager.

Determining the Status of Security Services

To determine whether security services are enabled for the current session, use the function **show_sec_services**. In the following example, the results indicate that unified login is enabled, and, therefore, so are the security services:

```
select show_sec_services()
 go
------------------------------------------------------
unifiedlogin
(1 row affected)
```

Configuration Parameters Used in Security Services

This section summarizes the configuration parameters that the unified login and security services use through LAN Manager. These parameters provide the following security checks:

- **msg integrity reqd** – to check data integrity
- **msg out-of-seq checks reqd** – to check message sequence
- **msg replay detection reqd** – to detect interception or replay
- **secure default login** – to specify a default login
- **unified login required** – to control user authentication

For general information on configuration parameters, see the *System Administration Guide*.

Checking Data Integrity

Summary Information	
Name in pre-11.0 version	N/A
Default value	0 (off)
Range of values	0 (off), 1 (on)
Status	Dynamic
Display level	Intermediate
Required role	System Security Officer

The **msg integrity reqd** parameter controls the checking of all messages to ensure data integrity. The **use security services** parameter must be set to 1 (enabled) for message integrity checks to occur.

Checking Message Sequence

Summary Information	
Name in pre-11.0 version	N/A
Default value	0 (off)
Range of values	0 (off), 1 (on)
Status	Dynamic

Summary Information	
Display level	Intermediate
Required role	System Security Officer

The **msg out-of-seq checks reqd** parameter controls the checking of all messages to ensure that the sequence is correct. The **use security services** parameter must be set to 1 (enabled) for sequence checks to occur.

Detecting Interception or Replay

Summary Information	
Name in pre-11.0 version	N/A
Default value	0 (off)
Range of values	0 (off), 1 (on)
Status	Dynamic
Display level	Intermediate
Required role	System Security Officer

The **msg replay detection reqd** parameter controls the checking of all messages to detect whether they have been intercepted (detect replay). The **use security services** parameter must be set to 1 (enabled) for replay detection checks to occur.

Specifying a Login

Summary Information	
Name in pre-11.0 version	N/A
Default value	0
Range of values	0 (followed by another parameter naming the default login)
Status	Dynamic
Display level	Intermediate
Required role	System Security Officer

The **secure default login** parameter specifies a default login for all users who are preauthenticated, but do not have a login in *master..syslogins*.

Use the following syntax to establish the secure default login:

```
sp_configure "secure default login", 0, default_login_name
```

where *default_login_name* is the name of the default login for a user who, although unknown to Adaptive Server, has already been authenticated by a security mechanism. This name must be a valid login in *master..syslogins*.

For example, to specify "dlogin" as the secure default login, execute:

```
select sp_configure "secure default login", 0,
  dlogin
```

Controlling User Authentication

Summary Information	
Name in pre-11.0 version	N/A
Default value	0
Range of values	0, 1
Status	Dynamic
Display level	Intermediate
Required role	System Security Officer

The **unified login required** parameter controls authentication of all users who log into Adaptive Server by means of a security mechanism. The **use security services** parameter must be set to 1 (enabled) to use the unified login security service.

Managing Login Security on an NT Computer

This section discusses how to use the login security features of Adaptive Server for Windows NT.

For more information on system security, see the *System Administration Guide*.

Note Adaptive Server also provides the capability to authenticate users through the NT LAN Manager. For more information, see Chapter 6, “Using Security Services with NT LAN Manager”.

Overview of Security Features

You can use Adaptive Server security features alone or in combination with the NT security features.

Adaptive Server Security

As a standalone product, Adaptive Server ensures security by:

- Storing login information for all database users in the *master.dbo.syslogins* table. Passwords stored are encrypted.
- Requiring client applications to specify the login name and password of a database user, either programmatically or with a command line option.
- Checking the username and password against the information in *syslogins*, and accepting or rejecting the login accordingly.

Combined Adaptive Server and NT Login Security

Adaptive Server increases security by integrating the default Adaptive Server login process with NT security features. The resulting integrated security modes add the following conveniences for users:

- Authorized users do not have to maintain separate login passwords for Adaptive Server and Windows NT.
- System Administrators can take advantage of NT security features such as encrypted passwords, password aging, domain-wide user accounts, and NT-based user and group administration.

Trusted Connections and Combined Login Security

Combined login security operates only over network protocols that support authenticated connections between clients and servers. Such connections are referred to as *trusted connections*.

Trusted connections are limited to client applications that access Adaptive Server by using the Named Pipes protocol.

Note Other network protocols, such as TCP/IP sockets and IPX/SPX, do not support authenticated connections, so clients on these protocols are handled according to the standard Adaptive Server login mechanism.

A System Administrator must use the **sp_grantlogin** system procedure to assign permissions to NT users and groups. Using **sp_grantlogin**, the System Administrator has the following additional options:

- Assigning one or more Adaptive Server roles to NT users and groups
- Designating that the user or group should receive the default database object permissions assigned by the **grant** command

If the System Administrator does not use **sp_grantlogin** to assign user or group permissions, users cannot log in through trusted connections. For more information, see “Permitting Trusted Connections” on page 107.

Note Adaptive Server does not permit trusted connections for NT users named “sa.” The username “sa” is reserved for the default Adaptive Server System Administrator account.

Understanding Login Security Modes

Adaptive Server provides the following modes for configuring login security:

- Standard
- Integrated
- Mixed

Standard Mode

When operating in Standard mode, Adaptive Server manages its own login validation process for all connections by:

- Ignoring the NT network username and checking the supplied Adaptive Server username and password against the information in the *syslogins* table
- Providing valid users with Adaptive Server connections and allowing valid users to receive the permissions and roles that were assigned to them with the **grant** command

For a description of the login security features of Adaptive Server, see the *System Administration Guide*.

Integrated Mode

When operating in Integrated mode, Adaptive Server uses NT-based authentication mechanisms for all connections by:

- Allowing only trusted connections, using Named Pipes, to connect to Adaptive Server
- Ignoring any Adaptive Server login name and password that is submitted in the login request. Instead, it checks the mapped NT network username against the information in the *syslogins* table.

  If no matching login name exists, and the login process includes a default username, Adaptive Server substitutes the default login name, for example, “guest”, to complete the connection. For more information, see “Default Login” on page 108.
- Providing authorized users, when they log in, with permissions and roles as described in “Permitting Trusted Connections” on page 107.
- Following the NT Domain structure for the use of computers. NT must authenticate each user, either through trust relationships or through explicitly assigned permissions on each server.

Note If you bypass the NT login security for Adaptive Server authentication, that is, if you opt for Adaptive Server security only, it does not matter to which user or group you assign the computers. The only requirement is that the protocol you use allows the client and server to communicate.

Mixed Mode

When operating in Mixed mode, Adaptive Server allows both trusted, as with Named Pipes, and "untrusted" connections. It first examines the requested login name as specified by the client application, then handles the login depending on the information supplied.

Adaptive Server processes the login:

- When the login name matches the mapped network username, is null, or is composed of spaces, Adaptive Server treats the login attempt as a trusted connection and uses the rules for Integrated mode.
- When the user supplies a different login name, Adaptive Server treats the login attempt as an untrusted connection and uses the rules for Standard mode.

Mixed mode offers users the convenience of login security integration without forcing all clients and applications to use that integration.

- Existing applications that embed a hard-coded login name and password for all users continue to operate as before.
- Other operating system clients, such as Apple Macintosh clients and UNIX-based workstations, also can access an Adaptive Server in Mixed mode.
- Users accessing Adaptive Server over trusted connections can avoid a separate Adaptive Server password validation by omitting the username and password in their login request.

Note Applications can be designed to send an empty login name field in the connection request, thereby avoiding a separate login step.

Managing the Login Security Features

Use the following elements to manage login security in Integrated or Mixed mode:

- Trusted connections
- NT Registry parameters

Permitting Trusted Connections

When operating under Integrated or Mixed Login Mode, Adaptive Server assigns permissions to trusted user connections by checking the user’s network or NT group name. This check determines whether the Security Administrator, using **sp_grantlogin**, has assigned an Adaptive Server role, or the **default** value, to that name, and Adaptive Server acts accordingly.

- When no permissions were assigned to the name, and Adaptive Server is operating in:
  - Integrated mode, Adaptive Server refuses the connection.
  - Mixed mode, Adaptive Server treats the connection as an untrusted connection. Then, the login process continues under the Standard mode rules.
- When one or more Adaptive Server roles have been assigned to the user’s network name or to the user’s NT group, the user receives those roles and permissions that were assigned by the Security Administrator through the **grant** statement.
- When only the **default** value has been assigned to the user’s network name or NT group, the user receives only the permissions and roles that were assigned by the Security Administrator through the **grant** statement.

The most important point to remember is that NT users or their associated NT groups must have permissions that were assigned with **sp_grantlogin**.

For examples of this system procedure, see “Assigning Trusted Connection Permissions” on page 111.

For more information about the **sp_grantlogin** procedure, see the *System Administration Guide*.

NT Registry Parameters

When you install Adaptive Server and other Sybase products on your computer, the installation program configures several parameters to help you to manage the login security features while in Integrated or Mixed mode.

This sections describes the following management parameters:

- Default Login
- Default Domain
- SetHostName

- Character Mappings

To modify the parameter values, see “Modifying the Parameter Values” on page 110.

Default Login

Adaptive Server uses the Default Login parameter to specify the Adaptive Server login name that an authorized user can enter when a network username does not appear in the *syslogins* table. Standard mode does not use this value.

When there is no value for Default Login, Adaptive Server denies access to users who do not have a network username in *syslogins*.

Default Domain

Adaptive Server uses the Default Domain parameter to specify the NT or LAN Manager domain name for matching network usernames to Adaptive Server login names.

Because two different domains can define the same network username for two different users, the following rules apply:

- Adaptive Server can authorize access to both distinct users, but it must be able to distinguish between the two names in the login process for a trusted connection.
- For usernames defined in domains other than the parameter’s default value, Adaptive Server adds the domain name and a domain separator, a backslash character (\), to the network username before looking for the username in the *syslogins* table.

Warning! The backslash character (\) is invalid for Adaptive Server. To avoid possible login name problems, you can map the backslash character to a valid Adaptive Server character. For more information, see “Character Mappings” on page 109.

For example, the domain MARKETING is the Adaptive Server default definition, and two different users employ the network username “john”, one in the MARKETING domain and the other in the ENGINEERING domain.

- John in MARKETING accesses Adaptive Server with the login name of “john” over a trusted connection.

  - John in ENGINEERING accesses the same Adaptive Server with a login name of “ENGINEERING\john” to which his name was mapped before the software looked it up in *syslogins*.

- When your server computer participates in a specific domain, set the Default Domain parameter to that domain name. Otherwise, set Default Domain to the server’s computer name.

SetHostName

The SetHostName parameter determines whether the host name from the client login record is replaced with the NT network username for users under integrated security mode.

- 1 (enabled) – to include the network username in the results of the **sp_who** system procedure.
- 0 (disabled) – the default, to omit the network username from the results of the **sp_who** system procedure.

To modify the SetHostName value, which is located in the following Registry path: *HKEY_LOCAL_MACHINE\SOFTWARE\Sybase\ Server\server_name*, you must use the **regedt32** utility.

For steps on using this utility with Adaptive Server, see steps 1-3 in “Increasing Windows Sockets Connections” on page 32.

For general information about **regedt32**, see your NT operating system documentation.

Character Mappings

Certain characters that are valid for NT usernames are not valid for Adaptive Server login usernames. Such characters include the following:

- Domain separator (\)
- Space ( )
- Hyphen (-)
- Period (.)
- Single quotation mark (’)
- Exclamation point (!)
- Percent sign (%)
- Caret (^)

- Ampersand (&)

Character mapping lets you determine how these invalid characters can be converted into characters that are valid for Adaptive Server.

For example, the NT username "t-johns" contains a dash character (-), which is invalid in Adaptive Server. You can map the dash character to a valid "at" sign (@) to make the username compatible with Adaptive Server, as "t@john". The mapping stores the dash as an "at" sign, but displays it as a dash.

When you first install Adaptive Server, the installation program maps a few invalid characters to the valid characters that are listed in Table 6-5.

Table 6-5: Default mapping values

Invalid Character	Valid Mapped Character
Domain separator (\)	Underscore (_)
Hyphen (-)	Pound sign (#)
Space ( )	Dollar sign ($)

Modifying the Parameter Values

To modify the values for the Default Login, Default Domain, and SetHostName parameters, use one of the following utilities, depending on your needs:

Note You can change the SetHostName value only through **reged32**.

- Use the Server Config utility to modify the value only for Adaptive Server.

  For general steps on using Server Config, see "Changing Login Security Options" on page 115.

- Use the **regedt32** utility to change the value directly for use throughout your NT operating system.

  For steps on using **regedt32** to affect your operating system, see your NT operating system documentation.

Administering Login Security Using System Procedures

You can administer integrated security under NT in the following ways:

- Assign trusted connection permissions – **sp_grantlogin**
- Display the current Registry values – **sp_loginconfig**

- Display permissions and usernames – **sp_logininfo**
- Revoke permissions – **sp_revokelogin**

For the full syntax for these procedures, see the procedure names in the *Adaptive Server Reference Manual*.

Assigning Trusted Connection Permissions

To assign permissions to NT users and groups that access Adaptive Server over trusted connections:

- Use **sp_grantlogin** when Adaptive Server is running under Integrated mode or Mixed mode, and the connection is Named Pipes.
- Use the **grant** command when Adaptive Server is running under Standard mode or Mixed mode with a connection other than Named Pipes.

The **sp_grantlogin** permissions can include either one or more Adaptive Server roles or just the **default** parameter. This parameter indicates that Adaptive Server provides the user with the default permissions as assigned by the **grant** command.

To use the **sp_grantlogin**, **grant**, and **default** parameters in an example:

1. To assign the System Administrator and System Security Officer roles to all members of the To use the sp_grantlogin, grant, and default parameters in an example
2. NT group named Administrators, enter:

   ```
   sp_grantlogin "Administrators", "sa_role sso_role"
   ```

3. Then, to assign “select” permissions on the *sales* table to the NT user, “hasani”, enter:

   ```
   sp_grantlogin "hasani", "default"
   grant select on sales to hasani
   ```

Note If you do not specify a role or a value with the **sp_grantlogin** procedure, the procedure automatically assigns the **default** value.

Displaying the Current Registry Values

To display the current settings for the Registry values, use **sp_loginconfig** as discussed under “NT Registry Parameters” on page 107.

For example, executing **sp_loginconfig** on a newly installed Adaptive Server displays a list similar to the following:

```
name                   config_item
 ---------------------- ----------------------
 login mode             standard
 default account        NULL
 default domain         EAST
 set host               false
 key _                  domain separator
 key $                  space
 key @                  space
key #                  -
```

Displaying Permissions and Usernames

To display the current permissions and mapped usernames for both NT users and groups, use **sp_logininfo**. The following list describes this sample display:

```
account name             mapped login name
        type                  privilege
          -------------- ---------------------------------------------
BUILTIN\Administrators   BUILTIN\Administrators
          group                      ‘sa_role sso_role oper_role’
WEST\chantal             WEST_chantal
           user                      ‘default’
EAST\chantal             chantal
          user                      ‘sa_role’
```

- Three roles were assigned to the NT administrators group: **sa_role**, **sso_role**, and **oper_role**.

  - The group names are prefaced by “BUILTIN\” to indicate that the entry refers to an NT group, rather than a username or Adaptive Server group.
  - The domain separator in a group name is not mapped to a valid Adaptive Server character.

  You do not need to add a login or grant further permissions to an NT group, but you do need to add a login for each user in that group.

- The first NT user, named “chantal,” has the **default** parameter assigned as a permission. “chantal” is a member of the WEST domain, and her mapped Adaptive Server login name is “WEST_chantal.”

  “WEST_chantal” is the name the System Administrator should use when assigning an Adaptive Server login name and permissions to this user.

- The second NT user, also named “chantal,” logs in from the EAST domain. Her mapped username is simply “chantal,” since EAST has been set as Adaptive Server’s default domain (see the second item in this list).

To change or revoke the displayed users, groups, and permissions use the **sp_grantlogin** and **sp_revokelogin** procedures.

Revoking Permissions Granted with *sp_grantlogin*

To revoke permissions that were granted with **sp_grantlogin** use either

- The **sp_revokelogin** command when Adaptive Server is running under Integrated Security mode or under Mixed mode, and the connection is Named Pipes.
- The **revoke** command when Adaptive Server is running under Standard mode or under Mixed mode, and the connection is other than Named Pipe.

The following command line revokes all permissions from the NT group named Administrators:

```
sp_revokelogin Administrators
```

Configuring Login Security

The section provides general guidelines and suggestions for configuring Adaptive Server login security. Although you can complete the configuration tasks in a variety of ways, it is easiest to follow the steps in the order shown.

Step 1: Create NT Users and Groups

To create the user accounts and user groups that will access Adaptive Server over trusted connections, run the User Manager from the Administrative Tools (Common) menu. To access this menu, Choose Programs from the Start menu.

Keep the following guidelines in mind when creating groups and users:

- Make sure that NT users and groups exist *before* you assign permissions to them in Adaptive Server.

- Be sure to create the accounts with a user name other than "sa".

Note Some functions that were assigned to the “sa” user in previous versions of Adaptive Server are now divided between the **sa_role** and **sso_role**. You may want to assign both roles to Adaptive Server system administrators to provide the same permission level on an upgraded system. For more information, see the *System Administration Guide*.

- Begin planning the permission levels you want to assign to the users and groups.

  Although it may seem intuitive to grant the **sa_role** to the NT Administrators group, the choice ultimately depends on the security requirements for your site.

When using integrated security features for the first time, consider restricting the permission level to a small group of NT users. After you become more experienced with administering integrated security, you can expand the permission levels to include NT groups.

Step 2: Configure Mapping and Default Domain Values

To set the mapping and Default Domain options, follow the instructions under “Changing Login Security Options” on page 115.

Be sure to configure these values *before* adding accounts to Adaptive Server in Step 4, as these values affect the format of entries in *syslogins*.

For example, a user named “joseph” in the WEST domain is to log into Adaptive Server over a trusted connection. If you set the Map_ value to the domain separator (\) and the Default Domain value to NULL, the name “WEST_joseph” must appear in the *syslogins* table. However, if you later change the Default Domain value to WEST, the login name “joseph” would need to be in *syslogins* instead of “WEST_joseph.”

Step 3: Set Login Security Mode

To set the security mode to either Integrated or Mixed, follow the instructions under “Changing Login Security Options” on page 115.

When using login security features for the first time, consider using Mixed mode. If, for some reason, you cannot connect over a trusted connection, Mixed mode allows you to log into Adaptive Server using standard Adaptive Server usernames and passwords, such as the username “sa”.

Step 4: Add Network Login Names to *syslogins*

To add a login name for each NT user who till access Adaptive Server over a trusted connection, use **sp_addlogin**. Remember to include any non-default domain names and the correct mapping characters in the login name.

If you are not sure what to enter as the login name, experiment with a sample user to clarify your options:

1. Use **sp_grantlogin** to assign a role to a sample user on the network.
2. Enter the **sp_logininfo** system procedure to determine what the format of entries in *syslogins* should look like.
3. Use the entries listed in the *mapped login name* column as templates for the login names you create with **sp_addlogin**.

Step 5: Assign Roles

To assign roles or "default" permissions to NT users or groups, use **sp_grantlogin**. When performing this step, keep in mind that assigning permissions to NT groups generally provides more flexibility than assigning permissions to individual users.

After you have configured several groups with the correct permissions, you can use the User Manager to manage individual user's access to Adaptive Server.

Changing Login Security Options

When you install a new Adaptive Server, the installation program sets it to operate in Standard mode. Use the Server Config tool to change the following settings:

- The login security mode (Standard, Integrated, or Mixed)
- The name of the default login account
- The name of the default domain
- Mapping values

To select a login security mode:

1. Log into Windows NT using an account with NT administrator privileges.
2. Start the Server Config utility.

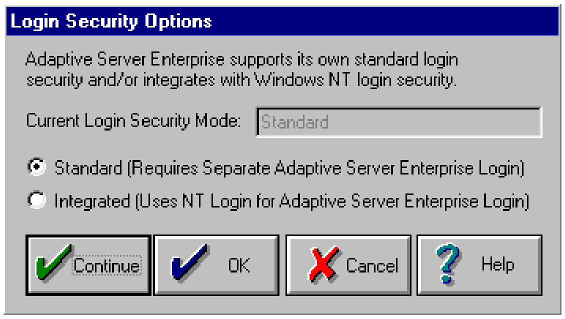
For instructions, see “Starting Server Config for Adaptive Server” on page 10.

3. Complete the initial steps to configure Adaptive Server.

   For instructions, see “Configuring Adaptive Server” on page 12.

4. Click the Login Security button in the Configure Adaptive Server Enterprise dialog box.

   Server Config displays the Login Security Options dialog box:



Login Security Options

Adaptive Server Enterprise supports its own standard login security and/or integrates with Windows NT login security.

Current Login Security Mode: Standard

● Standard (Requires Separate Adaptive Server Enterprise Login)

○ Integrated (Uses NT Login for Adaptive Server Enterprise Login)

5. Continue with For Standard Login Security Mode or For Integrated or Mixed Login Security Mode, depending on the login mode.

For Standard Login Security Mode

To enable Standard login security mode

1. Click the Standard option button to display Standard Current Login Security Mode box, then click OK.
2. Click Save in the Configure Adaptive Server dialog box.
3. Click Exit to quit Server Config.

For Integrated or Mixed Login Security Mode

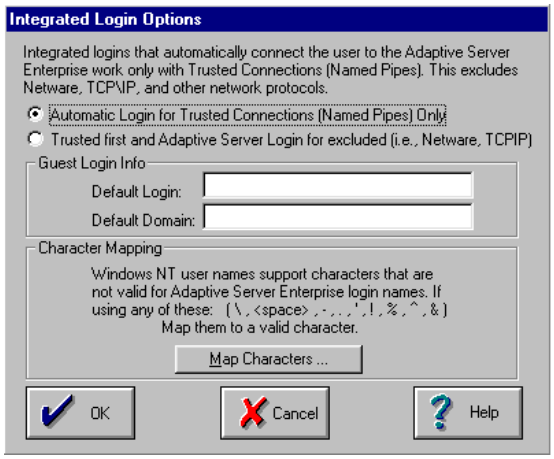
To enable Integrated or Mixed login security mode:

1. Click the Integrated option button to display Integrated in the Current Login Security Mode box, and click Continue.
2. Set the login security mode:

- For Integrated Mode, click the Automatic Login for Trusted Connections (Named Pipes) Only option.
- For Mixed mode, click the Trusted First and Adaptive Server Login for Excluded (i.e., Netware, TCPIP) option.

3. Enter the values to use as defaults:

    - In the Default Login box, type the name of the default user account to use for trusted connections.
      Adaptive Server uses this value when it cannot locate the username in *syslogins*. For more information, see “Default Login” on page 108.
    - In the Default Domain box, type either the default domain name or the workstation’s network name.
      For more information, see “Default Domain” on page 108.



Integrated Login Options

Integrated logins that automatically connect the user to the Adaptive Server Enterprise work only with Trusted Connections (Named Pipes). This excludes Netware, TCP\IP, and other network protocols.

● Automatic Login for Trusted Connections (Named Pipes) Only

○ Trusted first and Adaptive Server Login for excluded (i.e., Netware, TCPIP)

Guest Login Info

Default Login:

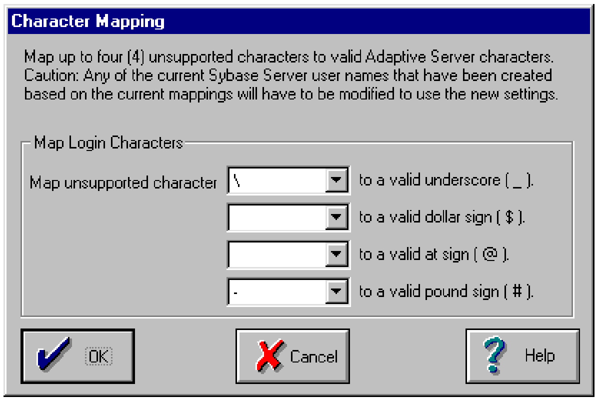
Default Domain:

Character Mapping

Windows NT user names support characters that are not valid for Adaptive Server Enterprise login names. If using any of these: (\ , <space> , - , . , ' , ! , % , ^ , &) Map them to a valid character.

4. Click the Map Characters button to configure Adaptive Server mappings under an Integrated security mode.

Server Config displays the Character Mapping dialog box.



Character Mapping

Map up to four (4) unsupported characters to valid Adaptive Server characters. Caution: Any of the current Sybase Server user names that have been created based on the current mappings will have to be modified to use the new settings.

Map Login Characters

Map unsupported character \ to a valid underscore (_).

to a valid dollar sign ($).

to a valid at sign (@).

- to a valid pound sign (#).

5. Use the drop-down lists to select the invalid character to be mapped to each valid Adaptive Server character.

   For more information, see “Character Mappings” on page 109.

6. Click OK to save the character mapping configuration and return to the Integrated Login Options dialog box.
7. Click OK in the Integrated Login Options dialog box.
8. Click OK in the Login Security Options dialog box.
9. Click Save in the Configure Adaptive Server dialog box to save the new configuration.
10. Click Exit to quit Server Config.

CHAPTER 7

Using E-mail with Adaptive Server

Adaptive Server can send and receive e-mail messages through Sybmail, the Sybase messaging facility, and can take advantage of NT Mail. This chapter provides instructions for using and configuring Sybmail to work with NT Mail.

Topics covered are:

Sybmail Messages

Adaptive Server for Windows NT can send, receive, and process e-mail messages.You can set Adaptive Server to manage these messages by using:

- A set of extended stored procedures (ESPs) that the user must run manually, or
- A system procedure that invokes the ESPs automatically by using procedural language code, rather than Transact-SQL statements.

Sending Messages

Messages from Adaptive Server (outgoing messages) can be one of two types:

- Text
- Formatted query results

Adaptive Server's capability for e-mail greatly increases the potential usefulness of a stored procedure or trigger. For example:

- A user-defined stored procedure that registers a new employee in the company database can include commands that send e-mail messages to a new employee and to other departments that need to be aware of the new hire, such as facilities, human resources, and training.
- A trigger on an inventory table can send an e-mail message to inform the purchasing department that an item needs to be reorder when an update causes the number of items on hand to fall below a certain level.
- A weekly report generated from a database query can be produced automatically and sent to a mailing list.

Receiving Messages

Adaptive Server's ability to process incoming mail allows users to send queries and receive results using e-mail, rather than a traditional client/server connection.

Sybmail flexibility allows a user to send queries to Adaptive Server from any computer, and, at a later time, to check e-mail for the results from either the same or a different computer.

Preparing NT Mail for Sybmail

Sybmail takes advantage of the NT Mail facility, so you need to prepare the NT Mail system before you can use Sybmail. You must:

1. Connect to a post office
2. Create a mailbox
3. Create a mail profile for Adaptive Server

The following sections provide a general outline for setting up Adaptive Server in the NT Mail system.

For detailed instructions on working with Mail on your system, see your NT operating system documentation or the *Microsoft Windows NT Resource Kit*.

Connecting to a Post Office

An NT post office holds messages until all of the recipients have retrieved them.

The computer that is running Adaptive Server must have access to an NT post office on the network. You can:

- Create a new post office, if one does not exist for your domain, or
- Connect to an existing workgroup post office.

When connecting to an existing post office, be prepared to supply its path.

Creating a Mailbox for Adaptive Server

After connecting to a post office, create a mailbox for Adaptive Server in the destination post office.

Note Only the NT post office administrator can add a new mailbox.

Be sure to supply a mailbox name and password for the mailbox.

- The password will be useful later when you establish a Sybmail user account on Adaptive Server.

  Make sure that the password meets the requirements for Adaptive Server passwords:

  - Must be at least 6 bytes.
  - Must be enclosed in quotation marks if the password does not begin with an alphabetic character.
- The mailbox name creates the association between the mailbox and the Adaptive Server mail profile that you will create in the next step.

Creating a Mail Profile for Adaptive Server

After you have added a mailbox for Adaptive Server, use the mailbox information to create a mail profile that is associated with the mailbox.

Note Each mail profile is associated with a single mailbox, although a single mailbox may be associated with several mail profiles.

The mail profile must have a password and be associated with a mailbox name.

- The password must be the same as Adaptive Server’s mailbox password.
- The mailbox name must be the same as the mailbox name specified when you created the mailbox for Adaptive Server.

In the Mail Login Properties window, make sure the checkbox labeled “When logging on, automatically enter password” is selected (checked).

Creating an Adaptive Server Login for Sybmail

After setting up an Adaptive Server profile in NT Mail, create a login for Sybmail on Adaptive Server. When creating this user account make sure that the following conditions are true:

- The *loginame* parameter is "sybmail".
- The *fullname* parameter has the same value as the Profile Name for Adaptive Server's mail profile.

  Adaptive Server uses this value as its MailUserName.
- The *password* parameter has the same value as the password for the mailbox that is associated with the server's mail profile.

  This value becomes Adaptive Server's MailPassword.

These values are the defaults for starting up an Adaptive Server mail session with the extended stored procedure **xp_startmail**, as discussed in "Managing a Mail Session" on page 126.

You can use either of the following methods to create a login for Adaptive Server:

- The **sp_addlogin** system procedure from **isql**:

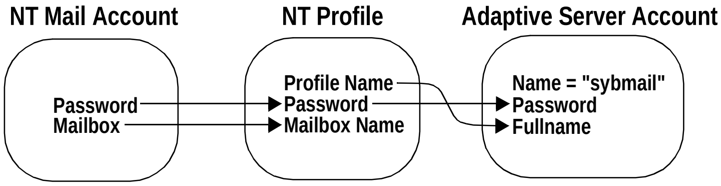
```
sp_addlogin "sybmail", "wrtyzz2c", @fullname="sqlserver"
```

  or

- The Add Login facility in Sybase Central or Adaptive Server Manager.

Figure 7-1 summarizes the relationships between the values that you supplied to prepare an account for Sybmail.

Figure 7-1: User-defined values relationships in Sybmail



Sybmail and Extended Stored Procedures

Adaptive Server uses XP Server, an Open Server application, to execute all of its extended stored procedures (ESPs), including the system ESPs that implement Sybmail.

By default, XP Server configuration uses the System Account (LocalSystem) as its start-up account. However, to use Sybmail, you must configure XP Server to start under a user account.

To configure XP Server for a user account:

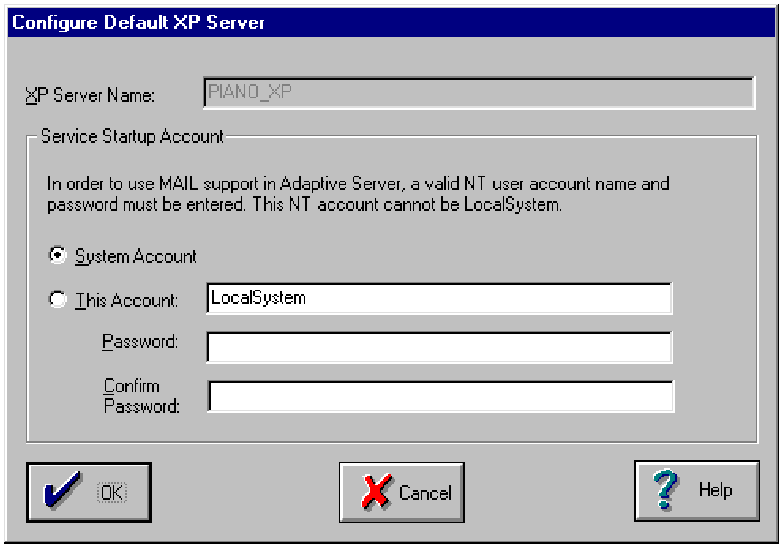
1 Start the Server Config tool.

For instructions, see “Starting Server Config for Adaptive Server” on page 10.

2 Complete the initial steps to configure Adaptive Server.

For instructions, see “Configuring Adaptive Server” on page 12.

3 Click the Configure Default XP Server button in the Configure Adaptive Server Enterprise dialog box.



Configure Default XP Server

XP Server Name: PIANO_XP

Service Startup Account

In order to use MAIL support in Adaptive Server, a valid NT user account name and password must be entered. This NT account cannot be LocalSystem.

● System Account

○ This Account: LocalSystem

Password:

Confirm Password:

4 Click This Account to enable the option, and type a valid NT user account and password for the server. Make sure that the account has the right to log in as a service. See steps a–f.

If you do not have an existing user account with the right to log in as a service, you can grant a user this right from the NT User Manager.

a Open User Manager from the Administrative Tools (Common) menu in the Start menu.

b Select the Username to act as the service.

c Choose User Rights from the Policies menu.

d In the User Rights Policy dialog box, select the Show Advanced User Rights check box.

e In the Right drop-down list, select "Log on as a service", and click OK.

f Exit the User Manager.

5 Click OK.

6 Click Save in the Configure Adaptive Server Enterprise dialog box.

7 Click Exit to quit Server Config.

Managing a Mail Session

You must initiate an Adaptive Server mail session before any messages can be sent or received.

Note Only one Sybmail session at a time can be running on an Adaptive Server.

Starting a Session

When Adaptive Server starts a session, the mail user is represented by the MailUserName and the MailPassword which you defined when you created the Adaptive Server login for Sybmail.

You can initiate an Adaptive Server mail session in one of two ways:

- Call the **xp_startmail** extended stored procedure explicitly each time you start Adaptive Server.

  You can override the previously mentioned login default by passing another username and password to **xp_startmail**. You might want to do this if there are multiple profiles associated with Adaptive Server's mailbox, and you want to use an alternative profile.

- Arrange to start a mail session automatically when Adaptive Server starts up.

  For automatic start-up of an Adaptive Server mail session for subsequent Adaptive Server sessions, set the **start mail session** configuration parameter to 1.

  With the automatic start-up, you do not need to use **xp_startmail** to begin a mail session the next time that you start Adaptive Server.

  For more information on **start mail session**, see the *System Administration Guide*.

Starting Sybmail Without Parameters

You can start Sybmail with **xp_startmail** and no parameters (default configuration), but only in the following situations:

- The Sybmail user account exists and the Start mail session parameter was configured to 1 when Adaptive Server was started, or

- The Sybmail user account exists, and you enter the following command to automatically start Sybmail:

  ```
  sp_configure "start mail session", 1
  ```

In both of these situations, do not restart XP Server before issuing the command to start Sybmail with its default configuration. Once you restart XP Server, it drops the default settings.

Stopping a Session

A mail session stops automatically when Adaptive Server shuts down. You also can explicitly stop an Adaptive Server mail session at any time with the **xp_stopmail** ESP.

For syntax and parameters for **xp_startmail** and **xp_stopmail**, see the *Adaptive Server Reference Manual*.

Note Be sure to stop the current Adaptive Server mail session with **xp_stopmail** before using **xp_startmail** to start another mail session for a different profile name. Until you stop the first session, the second session cannot access resources that are considered to be still in use by the first session.

Stored and Extended Procedures for Handling Messages

Table 7-1 summarizes the procedures that are available for processing e-mail for Adaptive Server.

Table 7-1: Procedures for processing mail

Procedure	Description
xp_deletemail	Deletes a message from the Adaptive Server message inbox.
xp_findnextmsg	Retrieves the message identifier of the next message in the Adaptive Server message inbox.
xp_readmail	Reads a message from the Adaptive Server message inbox.
xp_sendmail	Sends a message from Adaptive Server.
xp_startmail	Starts an Adaptive Server mail session.
xp_stopmail	Stops an Adaptive Server mail session.
sp_processmail	Reads, executes, responds to, and deletes messages submitted to Adaptive Server by e-mail.

Sending Messages

An outgoing message can consist of text or the formatted results of a query or batch of queries. You can send a message directly through **isql** from either a stored procedure or a trigger that uses the **xp_sendmail** ESP.

Keep the following concepts in mind when managing outgoing messages:

- To send query results, input the query, or a stored procedure containing the query, to **xp_sendmail**. The query results are sent to the recipients of the message.
- When the message consists of query results, you can specify whether you want the results to be sent in the body of the e-mail message or as an attachment.
- When the message consists of text, use the *message* parameter to **xp_sendmail**.
- When the message consists of the results of a query, use the *query* parameter, and pass the quoted text of the query or the quoted **execute** command with its stored procedure name.

For syntax and parameters for **xp_sendmail**, see the *Adaptive Server Reference Manual*.

Text Messages

The trigger in the following example sends e-mail to “purchasing” when an update causes the number of items on hand (*onhand*) in an inventory table (*part*) to fall below a certain level (*min_onhand*).

```
1> create trigger reorder
2> on part
3> for update as
4> if update(onhand)
5> if (select onhand - min_onhand
6> from inserted <= 0
7> begin
8> execute xp_sendmail
9> @subject="Inventory Notice"
10> @recipient="purchasing"
11> @message="Parts need to be reordered."
12> end
```

Query Result Messages

In response to the e-mail message generated by the trigger listed in the preceding Text Messages, the purchasing department can send the Adaptive Server mailbox a query to determine which parts should be reordered.

Note For a diagram of the process, see Figure 7-1 on page 123.

Adaptive Server then reads the query into a variable, named *received_mess*, as in the following example, with **xp_readmail**, and uses **xp_sendmail** to execute it and return the results:

```
declare @received_mess varchar(255)
execute xp_sendmail @recipient = "purchasing"
@query = @received_mess, @dbname = "inventory"
@dbuser ="sa"
```

Another example of mailing query results, a user-defined stored procedure, named **usp_salesreport**, in the *salesdb* database, is run at the end of the month to report on monthly sales activity. By invoking this procedure inside a call to **xp_sendmail**, you can automatically send the results of the procedure through e-mail to a mail group.

The following example sends the results of the **usp_salesreport** stored procedure as an attachment to an e-mail message addressed to “sales”, with copies to “mitchell” and “hasani”. The procedure is executed in the *salesdb* database with the privileges of the database owner of *salesdb*.

```
execute xp_sendmail @recipient = "sales",
@copy_recipient = "mitchell"; "hasani",
@subject = "Monthly Sales Report",
@query = "execute usp_salesreport",
@attach_result = true,
@dbname = "salesdb",
@dbuser = "dbo"
```

Receiving Messages

Adaptive Server expects incoming e-mail messages to be in the form of Transact-SQL statements. Incoming mail can consist of a single statement or a batch of statements, delimited by an end-of-batch indicator.

Note Messages containing multiple statements must follow the rules for batches, as described in the *Transact-SQL User's Guide*.

Sybmail provides ESPs to process incoming messages, including the following:

- **xp_findnextmsg**
- **xp_readmail**
- **xp_deletemail**

These ESPs are briefly described below. For syntax and parameters, see the *Adaptive Server Reference Manual*.

Finding the Next Message

xp_findnextmsg returns the message identifier of the next message in the Adaptive Server inbox. Use the **unread_only** parameter to specify the messages for consideration:

- **true** – to consider only unread messages
- **false** – to consider all messages

You need the message identifier that is returned by **xp_findnextmsg** to pass to subsequent procedures that read and delete messages.

Reading a Specific Message

You can read a specific message by passing its message identifier to **xp_readmail**.

To read the first message in the inbox, or the first unread message, depending upon the **unread_only** parameter, do not specify a message identifier.

xp_readmail places the contents of the message in its *message* output parameter.

Other output parameters that store the remaining attributes of the message include *originator* (message sender), *date_received* (message received date), *subject* (message subject), and *recipients* (message addressees).

Deleting a Message

After reading Adaptive Server's mail with **xp_readmail**, you can remove the message from Adaptive Server's inbox by passing the message identifier to **xp_deletemail**.

If you do not specify a message identifier, **xp_deletemail** deletes the first message in the inbox.

Processing Incoming Mail

You can process Adaptive Server's incoming e-mail queries manually by:

1. Calling the ESPs **xp_findnextmsg**, **xp_readmail**, and **xp_deletemail** individually for each message
2. Using **xp_sendmail** to execute the query in each message and send the e-mail results back to the requestor

However, it is much easier to use the **sp_processmail** system procedure, which invokes these ESPs automatically.

sp_processmail reads and responds to the unread messages in the Adaptive Server inbox. You can determine which messages to process by passing a value for the *originator* parameter and/or the *subject* parameter, as shown in Table 7-2.

Table 7-2: Selecting messages by sender or subject

When You Specify	sp_processmail Processes
originator	Only mail from the specified sender
subject	Only mail with the specified subject header
originator and *subject*	Only mail by the specified sender with the specified subject header
Neither *originator* nor *subject*	The unread mail in the inbox

sp_processmail uses default parameters when invoking **xp_sendmail**, but you can override the *dbname*, *dbuser*, and *separator* defaults by passing these values to **sp_processmail**. For the syntax for **sp_processmail** and **xp_sendmail**, see the *Adaptive Server Reference Manual*.

The following example processes all the unread mail sent to Adaptive Server by the e-mail sender "admin".

```
sp_processmail @originator = "admin",
@dbuser = "sa", @dbname = "db1"
```

The procedure executes the queries in the *db1* database in the System Administrator's context and returns the results an e-mail attachment to "admin" and to all the copied and blind-copied recipients of the original incoming message.

Using Sybmail Security

To prevent unauthorized users from accessing privileged Adaptive Server data through e-mail, you must set:

- The execution privileges on the ESPs that process mail
- The security context for executing queries

Use the **xp_sendmail** or **sp_processmail** procedures to set these values.

Setting Execution Privileges

The ESPs that process mail, such as **xp_findnextmsg**, **xp_readmail**, **xp_sendmail**, and **xp_deletemail**, are database objects owned by the System Administrator.

Limit execution permission of these procedures to users with the **sa_role** or to a very small group of users to prevent unauthorized users from accessing Sybmail to execute queries that they would normally not be able to execute.

Setting the Execution Context

When you use **xp_sendmail** to execute a query that has been submitted by e-mail, the procedure causes Adaptive Server to execute the query with the privileges of a particular Adaptive Server login in a particular database. This login/database combination is the *execution context*. By default, the login is “sybmail” and the database is “master.”

You can set the execution context for individual messages by passing different login and database values to **xp_sendmail** or **sp_processmail** with the following optional variables:

- *dbuser* – to reset the login name

  The login must represent a valid Adaptive Server account on the target Adaptive Server.
- *dbname* – to reset the database name

The following sections describe the execution context when the procedure specifies one, both, or neither of the optional variables.

Naming Both the User and the Database

Specify both *dbuser* and *dbname* to control how Adaptive Server executes the query. These variables can affect the process:

- In the user context of the specified login when that login is a valid user in the specified database
- In the user context of “guest” when the login is not a valid user in the specified database

When the specified database is a system database, a “guest” account always exists. However, when the specified database is a user database, the database owner must have ensured that:

- The entity represented by the *dbuser* login is a valid database user, or
- There is a “guest” user in the database that can map to any login and execute queries with minimal permissions.

Naming the User But Not the Database

Specify only *dbuser* to name a user but cause Adaptive Server to execute the command, **xp_sendmail** or **sp_processmail**, in the *master* database.

When the login specified by *dbuser* is not a valid user in the *master* database, Adaptive Server executes the query in the user context of “guest.”

Naming the Database But Not the User

Specify only *dbname* to set the default *dbuser* as “sybmail” and to cause Adaptive Server to execute any query under the user context of “guest.”

When the specified database is a system database, a “guest” account always exists. However, when the specified database is a user database, the database owner must have ensured that there is a “guest” user in the database that can map to any login and execute queries with minimal permissions.

Naming Neither the User Nor the Database

Specify neither parameter to retain the default *dbuser* as “sybmail” and the default database as *master*. Adaptive Server executes the e-mail query as “guest” in the *master* database.

CHAPTER 8

Managing Adaptive Server Databases

The administration of Adaptive Server databases includes both routine tasks and performance and tuning considerations.

- The *System Administration Guide* discusses most of the administrative tasks in detail.
- The *Performance and Tuning Guide* provides in-depth explanations of performance issues.

This chapter discusses some of the tasks described in these books that may require different handling for NT.

Topics covered are:

Managing Database Devices

The term *database device* refers to a disk or a portion of a disk that stores Adaptive Server databases and database objects.

Device Requirements

The size and number of Adaptive Server devices depend on the following constraints:

- The maximum device size is 8GB.
- Each database can have up to 128 devices.
- The maximum database size is 1TB.

Although some operating systems can designate an entire hard disk to use as a database device, Windows NT accepts only an operating system file (*.dat* file) as a database device.

When you install Adaptive Server, the program creates a *.dat* file in the *\data* directory of the Sybase installation directory. To use a *.dat* file as a database device, you can either use the default *d:\sybase\data* directory or create a device and a directory in which to store it.

Creating *.dat* Files for Database Devices

If you choose to create a new device, use the **disk init** command to specify the drive, path, and file name of the database device.

Warning! Do not place Adaptive Server devices on network drives, as this causes unpredictable system behavior. Also, if your Adaptive Server uses a network drive, you cannot start the server as an automatic NT service.

Example

To create a database device using the file *d:\devices\user1.dat*:

1. If the *d:\devices* directory does not exist, create it from the NT command prompt:

```
d:\> mkdir devices
```

2. Start **isql** and connect to Adaptive Server using the “sa” account:

```
d:\sybase\bin> isql -Usa -Ppassword -Sserver_name
```

3. Create the device using a **disk init** statement similar to the following example:

   ```
   1> declare @devno int
   2> select @devno = max(low/16777216)+1 from
   3> sysdevices
   4> disk init
   5> name = "user_device1",
   6> physname = "d:\devices\user1.dat",
   7> vdevno = @devno,
   8> size = 2048
   9> go
   ```

   The previous example creates a 4MB device, as measured in 2K pages, without an actual device number. To use a specific number, run **sp_helpdevice** to determine the number of an available device, and enter that number in place of **@devno**.

For more information about the **sp_helpdevice** system procedure and the **disk init** command, see the *System Administration Guide* and the *Adaptive Server Reference Manual*.

For more information about device files, see the *Performance and Tuning Guide*.

Note Raw partitions for database devices provide little performance advantage over files as database devices and might have been favored in past releases for cache coherence and security. However, because the Windows NT file system now addresses these concerns, it is recommended that you do not use raw partitions.

Backing Up and Restoring Data

Sybase supports tape drives and hard disks for backing up and restoring databases.

- The **dump** command backs up databases and transaction logs.

  To back up your databases, follow the instruction for "Using a Tape Drive" on page 138 or "Using a Hard Disk" on page 140, depending on which media you plan to use for the dump.

- The **load** command restores databases and transaction logs.

  To copy Sybase-supplied databases, see *Adaptive Server Enterprise Installation Guide for Windows NT*.

Note Always use the Adaptive Server **dump database** and **load database** commands, rather than the NT backup and restore utilities, to back up and restore Adaptive Server databases. Using the Adaptive Server commands ensures database integrity.

For more information about backing up and restoring databases, see the *System Administration Guide*.

Using a Tape Drive

Sybase software can back up and restore databases to tape drives that are compatible with Windows NT, including:

- 1/4-inch cartridge
- 4-mm and 8-mm digital audio tape (DAT) formats

To back up a database to a tape drive:

1. Install the tape drive according to the manufacturer's instructions.

   This task includes installing an NT-compatible driver for the tape drive by using the Add/Remove buttons in the Tape Devices dialog box from the Control Panel. For instructions, see your tape drive and NT operating system documentation.

2. Start **isql**, and connect to Adaptive Server:

   ```
   d:\sybase\bin> isql -Usa -Ppassword -Sserver_name
   ```

3. Use the NT tape device name with **isql** statements to name the tape drive.

For more information about using the **dump** and **load** commands, see "Examples of Backing Up and Restoring Databases" on page 141.

NT Tape Drive Names

Windows NT tape devices use the format "TAPE*n"*, where *n* is the tape drive number, in its physical device names. NT assigns the names as follows:

- TAPE0 is assigned to the tape drive with the lowest SCSI ID, then
- TAPE1 is assigned to the drive with the next highest SCSI ID, and so on until all devices have been assigned names

For example, to dump a database directly to the first tape drive, substitute the following value for the *stripe_device* parameter in the **dump database** command:

```
\\.\tape0
1> dump database pubs2 to "stripe_device"
 2> capacity = 10000
 3> go
```

The NT setup program uses these device names to create logical device names to refer to the NT tape devices; for example, *TAPEDUMP1* and *TAPEDUMPS2* (logical names) "for *TAPE0* and *TAPE1* (tape device names), respectively.

Note On your local computer, you can use the logical names *TAPEDUMP1* and *TAPEDUMP2* to refer to the associated tape devices. However, when you run the backup on a remote Backup Server, be sure to use the actual tape device names, rather than the logical names. See also "Setting the Maximum Capacity for a Tape Drive" on page 139.

To create a new, logical device name, use the **sp_addumpdevice** system procedure.

Setting the Maximum Capacity for a Tape Drive

To run properly, the **dump** command needs to know the maximum capacity of the destination tape drive. It determines this capacity in one of two ways, depending on the tape device name that you use:

- The physical device name – you must include the **capacity** parameter in the **dump** command. This parameter specifies the maximum number of bytes to write to a tape device.

Check your tape's capacity, and keep the following in mind:

- The minimum value that the **capacity** parameter can accept is 5 databases pages, 2K each.
- The maximum value that the **capacity** parameter can accept is 4,294,967,295K.
- The actual **capacity** value should be 70 to 80 percent of the true capacity of the tape.
- If you omit the **capacity** parameter for NT, Backup Server writes the maximum number of bytes for the specified tape device.

- The logical device name – the command uses the **size** parameter stored in the *sysdevices* system table.

  You can override that value by using the **capacity** parameter as described in the preceding list item.

Using a Hard Disk

Sybase software can back up data to any existing directory on a mounted NT volume.

To back up a database to a hard disk:

1. Select a volume that has enough free space to hold the database.
2. To place the database file in a new directory on the volume, use the **mkdir** command to create the directory.
3. Start **isql** and connect to Adaptive Server:

   ```
   d:\sybase\bin> isql -Usa -Ppassword -Sserver_name
   ```
4. Use the full drive, path, and file name designation to name the dump device.

For more information about using the **dump** and **load** commands, see "Examples of Backing Up and Restoring Databases" on page 141.

Dumping Across a Network

Backup Server may issue an "Access denied" message when you try to dump to a device mounted from across a network, particularly if you started Backup Server from Sybase Central.

By default, all NT services are started by using the "LocalSystem" user account, which does not allow the service to access network-mounted drives, for example, NFS, NetWare, or NTFS mounts from other machines.

To work around this restriction, configure Backup Server to start with a regular user account, rather than the NT default account. The user should have the permission to access remote drives.

To start Backup Server with a regular user account:

1 Double-click the Services icon from the Control Panel.

2 Select the Backup Server to configure, and click the Startup button.

3 In the Log On As area, name the user in the This Account box to activate that option, type the user's password, and confirm that password.

4 Click OK to exit the Services dialog box.

5 Click Close to exit Services.

Examples of Backing Up and Restoring Databases

Following are examples of using the **dump** and **load** commands for backup and recovery of Adaptive Server database on NT. For more information, see the *System Administration Guide* and the *Performance and Tuning Guide*.

User Databases

The following sections provide examples for backing up and restoring user database.

Specifying a Database and Device

This section provides examples on using a tape drive and a *.dat* file as the backup and recovery resources.

Using a tape drive

In the commands in this section, the physical device name *TAPE0* replaces the *stripe_device* variable.

To use the first tape device to back up and load a database:

```
1> dump database pubs2 to "\\.\TAPE0"
 2> go
1> load database pubs2 from "\\.\TAPE0"
 2> go
```

Using a *.dat* file

To back up and load the *pubs2* database using a *.dat* file:

```
1> dump database pubs2 to "d:\backups\backup1.dat"
2> go
1> load database pubs2 from "d:\backups\backup1.dat"
2> go
```

Specifying a Remote Backup Server

To back up to and restore from the first tape drive on a remote NT Backup Server named REMOTE_BKP_SERVER:

```
1> dump database pubs2 to "\\.\TAPE0" at REMOTE_BKP_SERVER
2> go
1> load database pubs2 from "\\.\TAPE0" at REMOTE_BKP_SERVER
2> go
```

Naming a Backup File

To back up a transaction log, the *syslogins* system table and create a default backup file name:

```
1> dump tran publications to "\\.\TAPE0"
2> go
```

To restore the log using the default file name in the **file** clause:

```
1> load tran publications from "\\.\TAPE0"
2> with file = "cations930590E100"
3> go
```

Note The **dump** command uses the last 7 characters in the database name *publications* to create the transaction log backup file *930590E100*. See the *System Administration Guide*.

In the following example, as directed by the user, the 15-character file name, *personnel97sep111800* records the following backup information:

- The database name (*personnel*)
- The date (*97sep11*) – September 11, 1997
- The time (*1800*) – 18:00 or 6:00 p.m

To back up the *personnel* database using the **file** clause to create the file name:

```
1> dump database personnel to "\\.\TAPE0"
2> with file = "personnel97sep111800"
3> go
```

To restore the *personnel* database by advancing the tape automatically to *personnel97sep111800* before restoring:

```
1> load database personnel from "\\.\TAPE0"
2> with file = "personnel97sep111800"
3> go
```

Note The file names in the preceding examples are valid only for systems that use the NTFS file system. If you are using a FAT-based file system, file names are limited to 8 characters with a 3-character extension.

Specifying Additional Dump Devices

To back up the database to three devices using the **stripe on** parameter and *three* devices:

```
1> dump database personnel to "\\.\TAPE0"
2> stripe on "\\.\TAPE1"
3> stripe on "\\.\TAPE2"
4> go
```

To restore the database using the **stripe on** parameter and *two* devices:

```
1> load database personnel from "\\.\TAPE0"
2> stripe on "\\.\TAPE1"
3> go
```

To back up a database using three devices, each attached to the remote Backup Server, REMOTE_BKP_SERVER:

```
1> dump database personnel
2> to "\\.\TAPE0" at REMOTE_BKP_SERVER
3> stripe on "\\.\TAPE1" at REMOTE_BKP_SERVER
4> stripe on "\\.\TAPE2" at REMOTE_BKP_SERVER
5> go
```

Tape Handling Options

To initialize two devices to overwrite the existing contents with the new transaction log backups:

```
1> dump transaction personnel to "\\.\TAPE0"
```

```
2> stripe on "\\.\TAPE1" with init
3> go
```

Getting Information About Files

To return header information for the first file on the tape:

```
1> load database personnel from "\\.\TAPE0"
2> with headeronly
3> go
```

To return header information for the file *personnel9229510945*:

```
1> load database personnel from "\\.\TAPE0"
2> with headeronly, file = "personnel9229510945"
3> go
```

System Databases

You can restore the following system databases:

- *master*
- *model*
- *sybsystemprocs*

For more information, see the *System Administration Guide*.

Optimizing Adaptive Server Performance and Tuning

You can make changes to your Windows NT system to improve Adaptive Server performance. The NT utilities let you monitor Adaptive Server's use of operating system resources—disk, memory, and I/O—to see if you need to make any changes to your system.

For more information, see the *System Administration Guide* and the *Performance and Tuning Guide*.

Using Dedicated Adaptive Server Operation

Installing Adaptive Server on a dedicated computer drastically improves performance, because the software does not have to share system resources with file and print server applications.

When you install Adaptive Server on a dedicated computer, set the default NT tasking option, to give the foreground application, in this case, Adaptive Server, the best application response time.

To set the default NT tasking option:

1. Log into NT using an account with NT administrator privileges.
2. Open the Control Panel.
3. Double-click the System icon.
4. Click on the Performance tab.
5. Click and drag the virtual lever to "Maximum" in the Application Performance area.
6. Click OK to apply the changes to your operating environment.
7. Close the Control Panel.

Using Disk Drives

The overall performance in an I/O-bound application is determined by the number of disk drives on a system, not by the amount of space available. A single disk drive might not be able to deliver the number of I/Os per second that are needed for your Adaptive Server application.

To achieve your performance objectives for an application, you must have enough disk drives to give the necessary number of I/Os per second.

Note Your disk drive requirements may not be directly related to the size of your database. Depending on the amount of I/O you need, you may have free space on your disk drives.

Monitoring Disk Usage

Sybase recommends that you distribute data in heavily used databases across multiple disks. To do this effectively, you need to monitor disk usage.

If one or more disks are consistently very busy, distribute the database objects on those disks to other devices. This strategy spreads out the work among disks and allow for greater data throughput.

You can use stored system procedures on Adaptive Server to monitor the disk space:

- To determine which devices a specific database is using, run **sp_helpdevice** or **sp_helpdb**.

  For more information, see **sp_helpdevice** and **sp_helpdb** in the *Adaptive Server Reference Manual*; also see the *System Administration Guide*.

- To check for disk space usage rates and I/O contention, run **sp_sysmon**.

  For more information, see **sp_sysmon** in the *Adaptive Server Reference Manual*; see also the *Performance and Tuning Guide*.

Monitoring Adaptive Server Statistics with NT Performance Monitor

You can use the NT Performance Monitor to monitor Adaptive Server statistics.

To support performance monitor integration, Adaptive Server must be registered as an NT Service. This registration occurs automatically in the following situations:

- When you start Adaptive Server through Sybase Central
- When you use the Services option through the Control Panel
- When you have configured NT to start Adaptive Server as an automatic service

To enable performance monitoring, make sure that the **SQL Perfmon Integration** configuration parameter is set to 1. If necessary, use the **sp_configure** system procedure to reset this parameter.

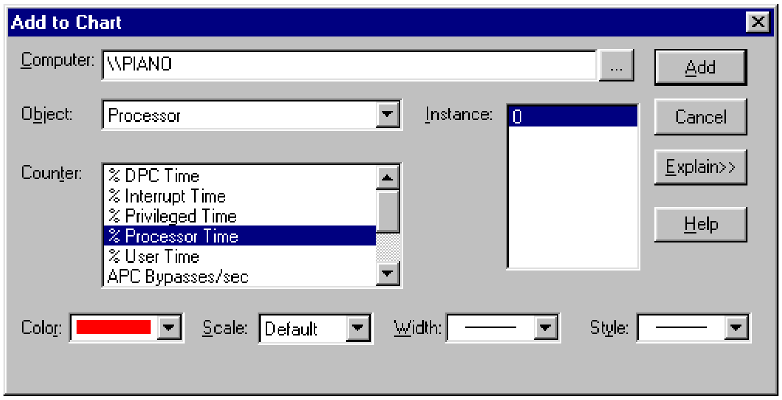
Note After you set this parameter, remember, you must restart Adaptive Server for the setting to take effect.

To monitor selected Adaptive Server statistics from NT Performance Monitor:

1 Start the NT Performance Monitor (*perfmon.exe*) from its program group.

2 Choose Add to Chart from the Edit menu.

The Add to Chart dialog box appears:



Add to Chart

Computer: \\PIANO

Object: Processor

Instance: 0

Counter:
% DPC Time
% Interrupt Time
% Privileged Time
% Processor Time
% User Time
APC Bypasses/sec

Color: 🟥

Scale: Default

Width: ———

Style: ———

3 Select the computer to monitor, if necessary.

- For a local computer, skip this step and go to step 4.
- For a remote computer, click the drop-down list button on the Computer text box, select the computer you are monitoring from the Select Computer dialog box, and click OK.

4. Select the Adaptive Server Counter group that contains the counter to monitor from the Object drop-down list.
5. Select the counter that you want to monitor from the Counter list for the selected group.

   For an explanation of a particular counter, select the counter and click the Explain button. The bottom of the dialog box displays the explanation.
6. If selecting a counter displays numbers in the Instance box, select the instance that you want to monitor.
7. Click Add to activate the counter on the Performance Monitor display.

For a list of Adaptive Server counters, see *Adaptive Server Enterprise Installation Guide for Windows NT*.

For general information on the NT Performance Monitor, see your NT documentation.

CHAPTER 9 Troubleshooting Network Connections

Net-Library enables clients and Adaptive Servers to interact with each other over a network. If the Net-Library software is not functioning properly, the client/server environment will not function properly either.

This chapter describes how to use the Ping Server option in the Directory Services Editor (**dsedit**) to get information about Adaptive Servers on a network.

Topics covered are:

The dsedit Server Ping Utility

Use the Directory Services Editor (**dsedit**) utility’s Server Ping utility to run tests on the Net-Library-to-server connections across your network software. The Server Ping utility reports information about both successful connections and failed connection attempts.

This test is particularly useful when you have multiple server names to identify more than one server in the *sql.ini* file.

You do not need to have a valid user name on Adaptive Server to run the Server Ping utility.

Running Server Ping

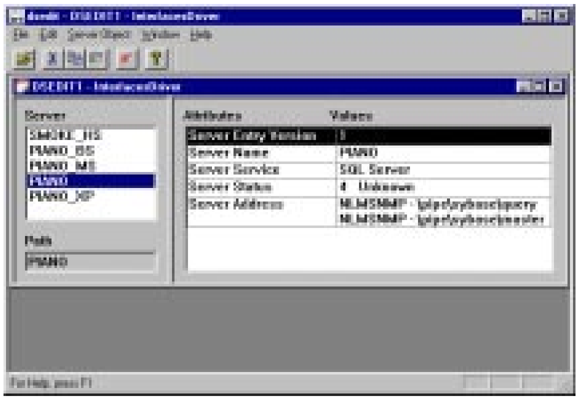
You can test the connections to any server that has a name in the *sql.ini* file on your client, as described in “How a Client Accesses Adaptive Server” on page 25.

To start the **dsedit** Server Ping option:

1 Start **dsedit**.

2 Select the directory service to open from the Select Directory Service dialog box, and click OK.

The Interfaces Driver dialog box for the server PIANO appears.


dsedit - DSEDIT1 - InterfacesDriver
File
Edit
Server Object
Window
Help
DSEDIT1 - InterfacesDriver
For Help, press F1

Server

- SMOKE_HS
- PIANO_BS
- PIANO_MS
- PIANO
- PIANO_XP

Path: PIANO

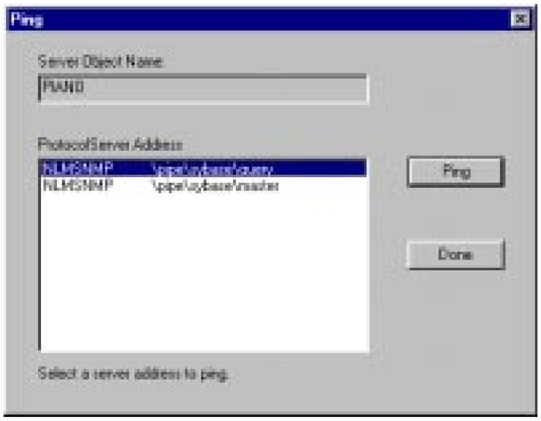
Attributes	Values
Server Entry Version	1
Server Name	PIANO
Server Service	SQL Server
Server Status	4 Unknown
Server Address	NLMSNMP - \pipe\sybase\query NLMSNMP - \pipe\sybase\master

3 Select the name of the server to test from the list of server names.

The server information displayed depends upon the specific Net-Library driver that you have installed.

4 Choose the Server Object menu, and choose Server Ping.

The Ping dialog box appears.



Server Object Name:
PIANO

Protocol/Server Address:

```
NLMSNMP      \pipe\sybase\query
NLMSNMP      \pipe\sybase\master
```

Select a server address to ping.

5 Click Ping to test the connection.

If Server Ping makes a successful connection to the server, a message indicating the success appears in a **dsedit** dialog box. A successful connection indicates that you have properly configured your Adaptive Server for network access.

If Server Ping reports an unsuccessful connection to the server, see “Troubleshooting Connection Failures” on page 152.

Troubleshooting Connection Failures

When a client application fails to connect to a server, you can test the application for diagnostic purposes. The messages that the Server Ping utility displays may provide you with enough information to solve the problem.

This test, however, cannot diagnose all types of network connection problems. Some problems may result from issues in your Adaptive Server setup, rather than in your Net-Library-to-network-software connection.

For tips on troubleshooting these setup problems, see “Failure of Other Applications” on page 154.

When a Test Fails

When Server Ping reports an unsuccessful connection, check to make sure the following Net-Library requirements have been met:

- Adaptive Server is running on the target server.
- A network hardware connection exists between your client machine and the target server.
- The server meets the minimum hardware and software requirements (see *Adaptive Server Enterprise Installation Guide for Windows NT*).
- The network software is installed and configured on the client and the server.
- The connection information in the *sql.ini* file is correct for the server.
- Check to ensure that the connection information in your client’s network configuration file(s) is correct. For more information, see the Net-Library documentation for your client.
- Make sure that the format of the connection information is correct for the network protocol. See“Components in the sql.ini File” on page 28.

If you need to edit *sql.ini*, use **dsedit**.

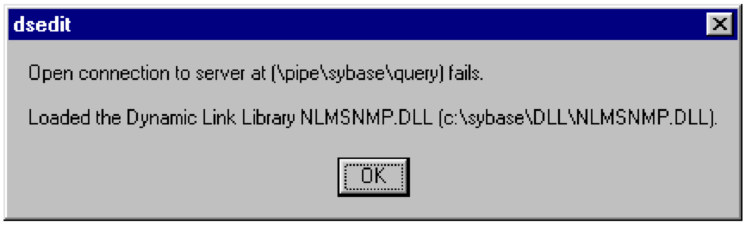
Warning! Make sure that no more than one copy of any Net-Library DLL is installed on your computer.

Using Returned Messages to Diagnose a Failure

When you are sure that the requirements named in “When a Test Fails” on page 152 have been met, determine the point at which the Server Ping failed by reviewing the resulting messages.

Failure to Connect to Adaptive Server

When Server Ping does not connect to a server, **dsedit** displays information about what went wrong. For example, if the server is not running, the message shown in this next screen might appear:



Open connection to server at (\pipe\sybase\query) fails.

Loaded the Dynamic Link Library NLMSNMP.DLL (c:\sybase\DLL\NLMSNMP.DLL).

Since it loaded the Net-Library DLL, **dsedit** found connection information in *sql.ini*. When the connection succeeds in finding the information, but notifies you that the server is not responding, you can use that information to discover the problem.

To troubleshoot an unsuccessful Server Ping:

1. Verify that the server is running.
2. Check that your networking software and hardware are properly configured.

   For example, check that your hardware connection has not been broken by loose connectors, plugs, and so on, and that your network software is running.
3. Check to see if any network error messages are displayed.
4. Check that the connection information is correct for your network protocol.

   For information on configuring the connection information for protocols included with Adaptive Server, see Chapter 3, “Setting Up Communications Across the Network”.
5. Make sure the format of your entries matches the format shown in Chapter 3, “Setting Up Communications Across the Network”.

Failure to Load Net-Library DLLs

Server Ping displays a message when it cannot load the Net-Library DLL. Check that the directory containing Net-Library DLL is included in the PATH environment variable.

Failure of Other Applications

When Server Ping reports no errors, but your other applications fail to run, use this information to discover the problem.

To troubleshoot a falsely successful Server Ping:

1. Verify that the Net-Library driver that you want to use is listed in the *libtcl.cfg* file.

   The utility does not look in *libtcl.cfg*, so Server Ping could be successful, even though the *libtcl.cfg* file contains incorrect information. The *libtcl.cfg* file is in the *ini* subdirectory of the Sybase installation directory.

2. Use **isql** to verify that you can access Adaptive Server locally from your computer.
3. Use **isql** to verify that the databases and tables used by your client application exist.
4. Verify that you have a valid user login name for Adaptive Server.
5. Verify that you have permissions on databases and tables that are consistent with the permissions required to run your applications.

Occasionally, a Server Ping result might indicate inaccurately a successful connection to Adaptive Server because **dsedit** found some other application listening at the specified Adaptive Server address. **dsedit** does not recognize that the non-Sybase application is not an Adaptive Server. To determine if this is the case, try to connect to the server with **isql**.

Before Calling Sybase Technical Support

For problems with your Net-Library application, have the following information available when you call Sybase Technical Support:

- The text of the diagnostic utility error
- A listing of your *sql.ini* file
- The name and version number of your network software
- The name and version number of the operating system on which your client and server networking software is running
- The version number of the server to which you are connected
- The date and size of your Net-Library DLL

  To locate this library information, execute the **dir** command to display a file list that includes the DLL.

APPENDIX A Adaptive Server Registry Keys

The Windows NT operating system stores configuration information in a tree-structured file called the Registry.

When you install Adaptive Server for Windows NT, the installation program and Server Config utility write configuration information to several branches, called *keys*, in the NT Registry.

This appendix presents the Registry values in a series of tables, one table for each key that appears under HKEY_LOCAL_MACHINE in the Registry:

- \SOFTWARE\SYBASE\Server\server_name   Table A-1
- \SOFTWARE\SYBASE\SQLServer\server_name\parameter   Table A-2
- \SOFTWARE\SYBASE\SQLServer   Table A-3
- \SYSTEM\CurrentControlSet\Control\Session Manager\Environment   Table A-4
- \SYSTEM\CurrentControlSet\Services\SYBSQL_server_name Table A-5

In some cases, you can use the information in this appendix to configure features of Adaptive Server. However, you can seriously impair your NT system if you make incorrect changes to the Registry.

Warning! Do not modify key values in the Registry unless you are an experienced NT administrator, and you are familiar with the **regedt32** utility. See your system NT documentation for information about using **regedt32**.

Table A-1: \SOFTWARE\SYBASE\Server\server_name

HKEY_LOCAL_MACHINE\SOFTWARE\SYBASE\Server\server_name			
Key Name	**Type**	**Default**	**Description**
DefaultDomain	REG_SZ	None	The default domain for mapping NT user names to Adaptive Server logins

HKEY_LOCAL_MACHINE\SOFTWARE\SYBASE\Server\server_name			
Key Name	**Type**	**Default**	**Description**
DefaultLogin	REG_SZ	None	The login ID to use for access to Adaptive Server when an authorized user does not have an Adaptive Server login defined in *syslogins*
LoginMode	REG_DWORD	0	The login security mode: • 0 indicates Standard • 1 indicates Integrated • 2 indicates Mixed
Map#	REG_SZ	Dash (-)	The special character mapped to the valid Adaptive Server pound sign (#) character
Map$	REG_SZ	Space ( )	The special character mapped to the valid Adaptive Server dollar sign ($) character
Map@	REG_SZ	Space ( )	The special character mapped to the valid Adaptive Server at sign (@) character
Map_	REG_SZ	Domain Separator (\)	The special character mapped to the valid Adaptive Server underscore (_) character
ServerType	REG_SZ	SQLServer	The type of server
SetHostName	REG_DWORD	0	Replacement status of the host name from the client login by the network user name under integrated security; • 1 = yes • 0 = no

Table A-2: \SOFTWARE\SYBASE\SQLServer\server_name\parameter

HKEY_LOCAL_MACHINE\SOFTWARE\SYBASE\SQLServer\server_name\parameters			
Key Name	**Type**	**Default**	**Description**
Arg0	REG_SZ	-d*d:\sybase\data\master.dat*	The location of the master device file
Arg1	REG_SZ	-s*server_name*	The name of the Adaptive Server
Arg2	REG_SZ	-e*d:\sybase\install\errorlog*	The location and name of the error log file
Arg3	REG_SZ	-i*d:\sybase\ini*	The location of the *sql.ini* file
Arg4	REG_SZ	-M*d:\sybase*	The directory that stores shared memory files

Table A-3: \SOFTWARE\SYBASE\SQLServer

HKEY_LOCAL_MACHINE\SOFTWARE\SYBASE\SQLServer			
Key Name	**Type**	**Default**	**Description**
CurrentVersion	REG_SZ	NT 11.5.1	The version number for the Adaptive Server software installed on the computer
DefaultBackupServer	REG_SZ	*server_name*_BS	The name of the default Backup Server

HKEY_LOCAL_MACHINE\SOFTWARE\SYBASE\SQLServer			
Key Name	**Type**	**Default**	**Description**
DefaultMonitorServer	REG_SZ	*server_name*_MS	The name of the default Monitor Server
DSEVNTLOG	REG_SZ	LocalSystem	The destination machine for logging messages to the NT event log
DSLISTEN	REG_SZ	*server_name*	The name Adaptive Server uses to listen for client connections when no name is given during Adaptive Server start-up
RootDir	REG_SZ	*D:\sybase*	The location of the Sybase installation directory for client applications to look for. Lists the SYBASE environment variable.
Version	REG_SZ	11.5.1	The version number of the Adaptive Server

Table A-4: \SYSTEM\CurrentControlSet\Control\Session Manager\Environment

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment			
Key Name	**Type**	**Default**	**Description**
DSLISTEN	REG_EXPAND_SZ	*server_name*	The name Adaptive Server uses to listen for client connections when no name is given during Adaptive Server start-up
DSQUERY	REG_EXPAND_SZ	*server_name*	The Adaptive Server name that client programs will try to connect to when no Adaptive Server name is specified in a command-line option
Path	REG_EXPAND_SZ	*current_path;d:\sybase\dll;D:\sybase\bin*	The NT path to which installation adds two paths to search for the Sybase *dll* and *bin* subdirectories
SYBASE	REG_EXPAND_SZ	*d:\sybase*	The Sybase installation directory for Adaptive Server and the Open Client/Server™ products

Table A-5: \SYSTEM\CurrentControlSet\Services\SYBSQL_server_name

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SYBSQL_server_name			
Key Name	**Type**	**Default**	**Description**
DisplayName	REG_SZ	Sybase SQL Server_ *server_name*	The Adaptive Server name used in the Services list under Control Panel
ErrorControl	REG_DWORD	0x1	For system use only
ImagePath	REG_EXPAND_SZ	*d:\sybase\bin\sqlsrvr.exe* -s*server_name* -C	The path for the Adaptive Server executable file
ObjectName	REG_SZ	LocalSystem	For system use only
Start	REG_DWORD	0x2	For system use only

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SYBSQL_server_name			
Key Name	**Type**	**Default**	**Description**
Type	REG_DWORD	0x10	For system use only

Index