SYBASE®
An SAP® Company

Configuration Guide

Adaptive Server® Enterprise 15.7 ESD #2

Windows

DOCUMENT ID: DC38421-01-1572-01
LAST REVISED: July 2012

Sybase, Inc., One Sybase Drive, Dublin, CA 94568.

Contents

CHAPTER 1 About Adaptive Server

Adaptive Server ® Enterprise 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 these auxiliary programs to perform dedicated tasks:

- Backup Server manages database load, dump, backup, and restoration activities.
- XP Server stores the extended stored procedures (ESPs) that allow Adaptive Server to run operating system commands.

Note: These instructions assume that Adaptive Server is installed and running. See the *Installation Guide* for your platform.

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 operating system that enable or enhance Adaptive Server performance
- Adaptive Server features that are available only on Windows
- 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

See the *Installation Guide* and release bulletin for your platform.

User Roles

The Adaptive Server setup process defines various user roles.

Different user roles have different responsibilities and privileges. These user roles clarify the way in which Adaptive Server is integrated into your system:

- Operating system administrator – the individual who maintains the operating system. This individual has administrator privileges.
- System administrator – the individual in charge of Adaptive Server system administration, creating user accounts, assigning permissions on databases, and creating new databases. At installation, the system administrator's login name is "sa". The "sa" login is specific to Adaptive Server and is used to log in to Adaptive Server using the **isql** command.

Environment Variables

It is crucial to the operation of Sybase® products that the system environment variables are set correctly. The installer sets the environment variables automatically at the system level.

As part of the installation, the installer sets up these environment variables:

- DSLISTEN – defines the name Adaptive Server uses to listen for client connections if no name is provided during the Adaptive Server start-up. If DSLISTEN is not set, and no name is given during the Adaptive Server start-up, the Adaptive Server name defaults to the server name given at installation.
- DSQUERY – defines the Adaptive Server name that client programs try to connect to if no Adaptive Server is specified with a command line option. If DSQUERY is not set, and you do not supply the Adaptive Server name with a command line option, clients attempt to connect to the server name given at installation.
- SYBASE – defines the path of the Sybase installation directory. The installation program sets up SYBASE to point to the release directory specified during installation.
- SYBASE_ASE – defines the subdirectory of the Adaptive Server components.
- SYBASE_OCS – defines the subdirectory to which Open Client™ is set.
- SYBASE_SYSAM – points to the license-management software directory.
- SYBASE_TS_MODE – on Windows, Adaptive Server uses SYBASE_TS_MODE to determine if the shared memory should use a Global namespace or a session-specific Local namespace. Sybase recommends that Adaptive Server use a Global namespace to which it can attach diagnostic tools for servers you start as a service, or when connecting to the server through terminal services.

  The default mode in versions of Adaptive Server earlier than 15.7 was Local, which imposed diagnostic limitations. In Adaptive Server 15.7 and later, the default is Global.

Setting SYBASE_TS_MODE to local starts Adaptive Server in pre- 15.7 default mode. There is no advantage in using a Local namespace and Sybase recommends that you do not do so, because it restricts shared memory access for diagnostic tools.

- PATH – specifies which directory paths to search for executables and dynamic link libraries (DLLs). The Sybase executables are in the `%SYBASE%|product_name\bin` directory. The installation program appends these paths to the current PATH environment variable.
- TEMP – defines the location used by the installation program to write files temporarily during the installation process. The installation process frees the disk space after installation is completed.
- INCLUDE – specifies which directory to set to or append for Open Client.
- LIB – is appended with `lib` directory for Open Client.

See also

- *Chapter 7, Start and Stop Servers* on page 19

CHAPTER 2 Adaptive Server Devices and System Databases

Devices are files or portions of a disk that are used to store databases and database objects. You can initialize devices using raw disk partitions or operating system files.

Adaptive Server requires these devices:

- `master` – to store system databases.
- `sybsystemdb` – to store information about transactions in process.
- `sysprocsdev` – to store system procedures.

The `master`, `sybsystemdb`, and `sysprocsdev` devices are created when you create a new Adaptive Server.

The master Device

The master device contains the `master`, `model`, `tempdb`, and sample databases.

- `master` – controls the operation of Adaptive Server and stores information about all users, user databases, devices, objects, and system table entries. The `master` database is contained entirely on the master device and cannot be expanded onto any other device.
- `model` – provides a template for new user databases. The `model` database contains required system tables, which are copied into a new user database with the **create database** command.
- `tempdb` – the work area for Adaptive Server. Each time Adaptive Server is started the `tempdb` database is cleared and rebuilt from the `model` database.
- The sample databases are stored on the master device at installation, but should be moved to a user-defined device after installation.

Note: For recovery purposes, Sybase recommends that you do not create other system or user databases or user objects on the master device.

The sybsystemdb Device

The sybsystemdb device stores the `sybsystemdb` database, which stores information about transactions in progress, and which is also used during recovery.

For instructions about creating the `sybsystemdb` device and database for distributed transaction management (two-phase commit), see *Upgrading Sybase Servers* in the *Adaptive Server Installation Guide* for your platform.

The sysprocsdev Device

The `sybprocsdev` devices stores the `sybsystemprocs` database, which contains most of the Sybase-supplied system procedures. System procedures are a collection of SQL statements and flow-of-control statements, for example **sp_configure**, that perform system tasks.

The system procedures that are needed during recovery situations are stored in the `master` database.

Note: `sysprocsdev` is the default system name for this device. However, it is frequently referred to as the `sybsystemprocs` device, since it stores the `sybsystemprocs` database.

Optional Devices and Databases

Optional devices and database include the PCI database, sample databases, the sybsecurity device and database, and the database consistency checker database.

Pluggable Component Interface (PCI) Database

The pluggable component interface (PCI) allows you to add libraries that provide different functionalities to the Adaptive Server. Java support (pluggable component adaptor/Java virtual machine) is included as a pluggable component with Adaptive Server 15.0.3 and later.

The `sybpcidb` database stores necessary configuration information for the PCI and the pluggable component adaptor/Java virtual machine (PCA/JVM) plug-in.

To enable PCI in Adaptive Server use the GUI utility **syconfig** or the command level utility **sybatch** .

When using **syconfig**, choose yes, for **Enable PCI in Adaptive Server**. Once enabled, the `sybpcidb` device path, device size, and `sybpcidb` database size must be configured. See "Managing Java in the Database During Installations and Upgrades," in the *Adaptive Server Enterprise Installation Guide for Windows*.

When using **sybatch**, add PCI/Java related properties to the resource files used by these utilities. Enter these values:

```
sqlsrv.do_configure_pci: yes
sqlsrv.sybpcidb_device_physical_name:\device_path
sqlsrv.sybpcidb_device_size: USE_DEFAULT
sqlsrv.sybpcidb_database_size: USE_DEFAULT
```

Sample Databases

The pubs2, pubs3, interpubs, and jpubs are the sample databases.

- pubs2 and pubs3 are provided as learning tools for Adaptive Server. pubs2 is used for most of the examples in the Adaptive Server documentation; other examples use the pubs3 database. Both are available in U.S. English versions of Adaptive Server.
- interpubs database contains French and German data.
- jpubs contains Japanese data.

For information about installing the sample databases, see *Post-Installation Tasks* in the *Adaptive Server Installation Guide* for your platform.

For information about the contents of the sample databases, see the *Transact-SQL Users Guide*.

sybsecurity Device and Database

The sybsecurity device is created as part of the auditing installation process. The sybsecurity device stores the sybsecurity database and the auditing system procedures with which you can configure auditing for your system.

The auditing system records system security information in an Adaptive Server audit trail. You can use this audit trail to monitor the use of Adaptive Server or system resources.

For information about installing and using the auditing system, see *Auditing* in the *System Administration Guide: Volume 1*.

See also

- *Chapter 17, Database Management System Auditing* on page 139

dbccdb Database

The database consistency checker (**dbcc**) provides commands for checking the logical and physical consistency of a database. The dbccdb database stores the results of **dbcc** when **dbcc checkstorage** or **dbcc checkverify** is used.

dbcc checkstorage records configuration information for the *target database*, operation activity, and the results of the operation in the dbccdb database. Stored in the database are **dbcc** stored procedures for creating and maintaining dbccdb and for generating reports on the results of **dbcc checkstorage** operations.

See *Checking Database Consistency* in the *System Administration Guide: Volume 2*.

Using Operating System Files as Database Devices

For devices that are initialized on operating system files, ensure that device writes occur directly on the physical media.

Use:

- **directio** with **disk init** and **disk reinit**
- **dsync** with **disk init**

directio and **dsync** parameters are mutually exclusive. If a device has **dsync** set to true, you cannot set **directio** to true for this device. To enable **directio** for a device, also reset **dsync** to false.

There is no performance difference between **dsync** and **directio** on Windows.

The dsync Parameter

The **dsync** parameter ensures Adaptive Server can recover data from devices on file systems.

By default, Adaptive Server disables **dsync** for file system devices. You can set or reset **dsync** using the **disk init** and **disk reinit** commands. When **dsync** is set to false (off), cached I/O is used.

Note: dsync and **directio** are ignored for raw devices.

Immediately after upgrading, check that either **dsync** or **directio** is set for the file system devices. See also **sp_helpdevice** in the *Reference Manual: Procedures*

The directio Parameter

The **directio** parameter for **disk init** and **disk reinit**, lets you bypass the operating system buffer cache and transfer Adaptive Server data directly to disk.

directio performs I/O in the same manner as raw devices and provides the same performance benefit, but has the ease of use and manageability of file system devices.

By default, the **directio** option is set to true (on) for all platforms. **directio** and **dsync** are ignored for raw devices.

See the *System Administration Guide, Volume 1.*

CHAPTER 3 Client/Server Communication

Adaptive Server communicates with other Adaptive Servers, Open Server applications (such as Backup Server), and client software on your network. Clients can interact with one or more servers, and servers can communicate with other servers by remote procedure calls.

For Sybase products to interact with one another, a directory services file must list the names and addresses of every known server. This information can be stored in either:

- An interfaces file called `sql.ini` on Windows platforms, located in the %SYBASE% `\ini` installation directory, or
- An LDAP server

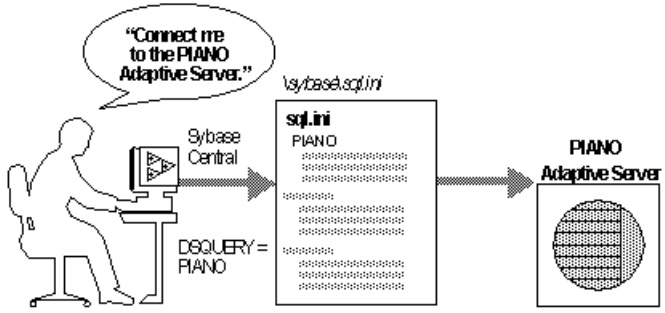
After your Adaptive Server or client software is installed, it can connect with any server on the network that is listed in the interfaces file or in the LDAP server.

When you are using a client program, and you want to connect with a particular server, the client program looks up the server name in the interfaces file and connects to that server. You can supply the name of the server by using the DSQUERY environment variable.

On TCP/IP networks, the port number gives clients a way to identify the Adaptive Server to which they want to connect. It also tells Adaptive Server where to listen for incoming connection attempts from clients. Adaptive Server uses a single port for these two services (referred to as *listener service query service*).

On SPX networks, the socket number gives clients and servers a way to identify each other.

Figure 1: Communicating with a Server Using the sql.ini File



The installer adds entries to the `sql.ini` file for the new Adaptive Server, Backup Server, or XP Server.

Note: You can use Windows File Replication to replicate `sql.ini` in the multiple locations. See the Microsoft documentation for information. You can also use Windows Registry to keep the interfaces file information.

CHAPTER 4 About Changing Adaptive Server Configurations

You may need to change the default Adaptive Server configuration to your specifications.

Changing the Adaptive Server configuration may include:

- Adjusting to your system's needs.
- Configuring languages, character sets, and sort orders.
- Using high availability features. See *Using Sybase Failover in a High Availability Environment*.
- Using distributed transaction management (two-phase commit). See the *Distributed Transaction Management User Guide*.

See also

- *Chapter 9, Adaptive Server Configurations* on page 27
- *Chapter 12, Localization Support* on page 57

CHAPTER 5 Languages Other Than US English

Many configuration tasks require the use of the Server Config utility.

If you are running Server Config in a language other than US 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 Installation Guide* for your platform.

CHAPTER 6 Adaptive Server Specifications

Adaptive Server specifications include databases, tables, queries, procedures, and extended-limit capabilities information about Adaptive Server requirements.

Database Specifications

Database specifications define requirements for items such as database size, and the number of database devices per server.

Item	Requirement	Notes
Databases per Adaptive Server	A maximum of 32,767 databases per server	
Maximum database size	• 2K page server – 8TB • 4K page server – 16TB • 8K page server –32TB • 16K page server – 64TB	
Minimum allowable `sybsystemprocs` database	136MB	Required for an upgrade
Maximum size of a database device (disk partition)	2^{42} (4TB)	If the operating system supports file sizes up to 4TB, then Adaptive Server supports file system devices up to 4TB
Maximum number of database devices per server	2^{31}	
Maximum number of devices or device pieces per database	Unlimited	Limited by available memory
Maximum number of segments per database	31	
Maximum number of login IDs per serve	2147516416	
Maximum number of users per database	2146484223	
Maximum number of groups per database	1032193	

Table Specifications

Table specifications defines requirements for items such as indexes, rows, and columns per table.

Item	Requirement	Notes
User objects per database	$2^{31} – 255$	
Indexes per table	250 (one clustered index)	
Rows per table	Limited by available storage	Maximum 2^{32}
Columns per composite index	31	
Creation of clustered index	1.2*(x + y) x = total data space in table, y = sum of space of all nonclustered indexes on table, and 20 percent overhead for logging	For sorted data, approximately 20 percent of the table size needed
Maximum size of object name	255	

Query Specifications

Query specifications define requirements for items such as maximum number of tables in a "union" query.

Item	Requirement	Notes
Maximum number of: • tables participating in a query • a query without a union, or, • each side of a union in a query	64	Maximum of: • 50 user tables – including result tables, tables referenced by views (the view itself is not counted) correlations and self-joins • 46 worktables
Maximum number of tables in a “union” query	256	Includes up to 50 user tables and 14 worktables on every side of the union, for a maximum of 256 tables across all sides of the union

Item	Requirement	Notes
Maximum number of databases participating in one transaction	Unlimited	Includes database where transaction began, all databases changed during transaction, and `tempdb`, if it is used for results or worktables
Practical number of databases participating in one query	16	Includes each occurrence of each database queried and `tempdb`, if it is used for results or worktables
Maximum number of tables with referential integrity constraints for a query	192	

Procedure Specifications

Procedure specifications list items such as number of buffers and procedure buffers, and the required minimum memory per stored procedure.

Item	Requirement	Notes
Number of buffers and procedure buffers	Configurable	Limited by amount of RAM and maximum size of shared memory segment
Minimum memory required per stored procedure	2K	
Maximum number of parameters per stored procedure	2048	

Extended-Limit Capabilities

Adaptive Server extended-limit capabilities vary by type of table and the database logical page size.

Allpages-Locked (APL)Tables

Maximum APL table limits	Number of columns	Column size 2K page	Column size 4K page	Column size 8K page	Column size 16K page
Fixed-length column	1024	1960 bytes	4008 bytes	8104 bytes	16296 bytes

Maximum APL table limits	Number of columns	Column size 2K page	Column size 4K page	Column size 8K page	Column size 16K page
Variable-length column	254	1948 bytes	3988 bytes	8068 bytes	16228 bytes

Data Row and Data Page Tables for Data-Only-Locked (DOL) Tables

Maximum DOL table limits	Number of columns	Column size 2K page	Column size 4K page	Column size 8K page	Column size 16K page
Fixed-length column	1024	1958 bytes	4006 bytes	8102 bytes	16294 bytes
Variable-length column	1024	1954 bytes	4002 bytes	8098 bytes	16290 bytes

Database Requirements for Varying Page Sizes

Database space requirements depend on the logical page size of the server. If your `model` database is larger than the minimum size listed below, then the minimum size of the database is equal to the `model` database.

Databases	2K page	4K page	8K page	16K page
Default database size	3MB	6MB	12MB	24MB
`master` database	13MB	26MB	52MB	104MB
`model` database	3MB	6MB	12MB	24MB
`tempdb` database	4MB	6MB	12MB	24MB
`sybpcidb` database	24MB	48MB	96MB	192MB

Data Limits for Tables According to Page Size

Larger logical page sizes can contain more data.

Tables	2K page	4K page	8K page	16K page
Bytes per index key	600	1250	2600	5300
User-visible row length DOL table	1958	4006	8102	16294
User-visible row length APL table	1960	4008	8104	16296

CHAPTER 7 Start and Stop Servers

Start and stop Adaptive Server and Backup Server after a shutdown for database maintenance, because of an operating system failure, or for other reasons.

XP Server is not started by the installation process. XP Server is started only when any XP command is issued through **isql**.

You can use Sybase Control Center to start and stop servers manually or automatically. The ASE plug-in can also start Adaptive Servers monitored by Unified Agent if the agent is properly configured.

To start a server, your user account must have:

- Windows administrator privileges
- Access to the Adaptive Server distribution files
- Access to a `sql.ini` file entry for the server
- System environment variables set correctly
- Access to SySAM licenses. See the *Sybase Software Asset Management Users Guide*.

The installation program creates the `sql.ini` file and system environment variables when you install servers on your computer.

See also

- *Environment Variables* on page 2

Server Start-up Parameters

Adaptive Server and Backup Server store their default start-up parameters in the Windows Registry file. This allows you to start and manage servers as Windows services, and allows servers to start automatically when you start your computer.

The default start-up parameters are stored under the Registry key \ \HKEY_LOCAL_MACHINE\SOFTWARE\SYBASE\Server\ *server_name*\Parameters, where *server_name* is the name of the server you installed. Backup Server server names are appended with "_BS".

Note: You can install multiple servers, each with its own Registry key.

Start-up parameters are listed under Registry values named `Argn`, where *n* is a number from 0 to 8. The number of the argument indicates the order in which the server reads the parameter.

Table 1. Default Adaptive Server Start-Up Parameters

Parameter	Switch	Description
`Arg0`	`-d %SYBASE%\data\mas-ter.dat`	Location of the master device file
`Arg1`	`-s server_name`	Name of the Adaptive Server
`Arg2`	`-e%SYBASE%\%SYBASE_ASE%\ install\errorlog`	Location and name of the error log file
`Arg3`	`-i %SYBASE%\ini`	Directory containing the `sql.ini` file
`Arg4`	`-M %SYBASE%\%SYBASE_ASE%`	Directory that stores shared memory files
`Arg5`	`-N%SYBASE%\$SYBASE_ASE%\ sysam \<srv_name>.properties`	Location and name of license cache file

You cannot change any of these default start-up parameters unless you directly edit the Windows Registry values. However, you can use Server Config to specify additional start-up parameters.

Specifying Additional Start-up Parameters

Additional start-up parameters include any valid server command line options listed for the **sqlsvr** and **bcksrvr** descriptions.

1. Log in to Windows using an account with Windows administrator privileges.
2. Start Server Config at **Start > Programs > Sybase > Adaptive Server Enterprise > Server Config**.
3. Select the **Adaptive Server** or **Backup Server** icon to indicate the type of server to configure.
4. Select **Configure Adaptive Server** or **Configure Backup Server** to display a list of available servers on your system.
5. Select the name of the server to configure, and choose **Continue**.
6. If you are configuring Adaptive Server, enter the login name and password of a user with system administrator privileges, and choose **Continue**.
7. If Adaptive Server is not running, Server Config asks you to start it now; choose **Yes**.
8. Select **Command Line**.
9. Edit the text in the Command Line Parameters box to include the additional start-up parameters and values you require.

Do not specify the default command line parameters. For details about available command line parameters, see **sqlsvr** and **bcksrvr** in the *Adaptive Server Utility Guide* for your platform.

10. Choose **OK**.
11. Choose **Save** in the server's configuration dialog box.
12. Exit Server Config.

Starting and Stopping Servers Using Unified Agent

You can start and shut down local or remote Adaptive Servers running if you have the proper permission to do so.

1. From the ASE plug-in, connect to the Adaptive Server to shut down.
2. Select **File > Shutdown**.

   If the Adaptive Server is monitored by Unified Agent, you do not have to connect first. Simply select the Adaptive Server and then select **File > Shutdown**.

Start and Stop Servers Using the Control Panel

You can start, stop, and pause a server both automatically and manually from the Services applet in the Control Panel.

Note: If you are running Adaptive Server and the Windows Process Viewer, and Adaptive Server is listed in the Process Viewer, you may not be able to restart Adaptive Server after you shut it down. This is because the Process Viewer holds some Registry resources, even after the viewed process is closed. Shut down the Process Viewer before you restart Adaptive Server.

Starting Servers as an Automatic Service

You can configure your operating system for automatic restart of Adaptive Server and Backup Server.

In production systems, Adaptive Server and Backup Server should start automatically when you restart your computer.

Note: Do not place Adaptive Server devices on network drives. If Adaptive Server uses a device on a network drive, you cannot start the server as an automatic Windows service.

Setting Up Adaptive Server as an Automatic Service

Use the Control Panel to set up the server as an automatic service.

1. In Windows Services at **Start > Settings > Control Panel > Administrative Tools > Services**.

2. Scroll through the list of available services until you find the listings for your Sybase servers.

   Server names use this format:

   Sybase *type*Server _ *servername_suffix*

   where *servername* is the name of the Adaptive Server and *type* and *_suffix* represent the server type:
   - SQL – Adaptive Server
   - BCK and _BS – Backup Server
   - XP and _XP – XP Server
3. Double-click Adaptive Server, or right-click Adaptive Server service entry and select **Properties**.
4. Select **Automatic** as the start-up type.
5. Click **Close**.

The selected server now starts automatically each time you restart the computer. You can verify the status of the server by examining the **status** column in the Services applet.

See your Windows documentation or online help for more information about setting up automatic services.

Starting, Stopping, and Pausing Servers Manually

Use the Control Panel to manually stop, start, and pause Adaptive Server.

1. Log in to Windows using an account with Windows administrator privileges.
2. Choose **Start > Settings > Control Panel > Administrative Tools > Services**.
3. Scroll through the list of available services until you find the listings for your Sybase servers.

   Server names use this format:

   Sybase *type*Server_*servername_suffix*

   where *servername* is the name of the Adaptive Server and *type* and *_suffix* represent the server type:
   - SQL – Adaptive Server
   - BCK and _BS – Backup Server
   - XP and _XP – XP Server
4. Select the service name, then click **Start**, **Stop**, or **Pause** to confirm the choice.
5. Click **Close**.

You can verify the status of the server either by using Sybase Central or by examining the `status` column in the Services applet.

Stopping Backup Server

Only the system administrator has permission to issue a **shutdown** command. Using a **shutdown** command minimizes the amount of work for automatic recovery when the servers are restarted. The preferred method of stopping Backup Server is to use the Transact-SQL™ **shutdown** command.

1. Log in to a server with system administrator privileges:
   ```
   isql -Usa -Ppassword -Sserver_name
   ```
2. Enter:
   ```
   1> shutdown SYB_BACKUP
   2> go
   ```

After you shut down a Backup Server, you must wait at least 30 seconds before restarting it.

A message similar to this prints to the `stderr` file:

```
Backup Server: 3.48.1.1: The Backup Server will go down immediately.
 Terminating sessions.
```

This is normal behavior. If a message indicates that Adaptive Server or Backup Server is waiting for processes to complete, and you must stop Adaptive Server or Backup Server immediately, you can use the **shutdown with nowait** command. **shutdown with nowait** does not wait for currently executing statements to finish and does not perform checkpoints in every database. Using **shutdown with nowait** for Backup Server may cause inconsistent or incomplete dumps and loads. Use this command only when necessary.

For more information on the **shutdown** command, see the *Reference Manual: Commands*.

Stopping Adaptive Server

Only the system administrator can issue a **shutdown** command. Using a shutdown command minimizes the amount of work that automatic recovery needs to do when the servers are restarted. The preferred method of stopping Adaptive Server is to use the Transact-SQL **shutdown** command.

1. Log in to an Adaptive Server account with System Administrator privileges:
   ```
   isql -Usa -Ppassword -Sserver_name
   ```
2. Enter:
   ```
   1> shutdown
   2> go
   ```

The default for the **shutdown** command is **with wait**. The **with wait** option allows Adaptive Server to finish executing SQL statements or procedures, perform a checkpoint in each database, disable new logins, and perform other shutdown tasks.

A message similar to this prints to the `stderr` file:

```
Server SHUTDOWN by request. The SQL Server is terminating this
process.
CT-LIBRARY error:
```

This is normal behavior.

If the message indicates that Adaptive Server is waiting for processes to complete, and you must stop Adaptive Server immediately, you can use the **shutdown with nowait** command. **shutdown with nowait** does not wait for currently executing statements to finish, nor does it perform checkpoints in every database. Use the **shutdown with nowait** command only when necessary.

CHAPTER 8 Monitor Servers

Use Unified Agent or the Control Panel to check a server's status.

You can monitor the Adaptive Server status either locally or remotely using Unified Agent.

For more information about using Unified Agent to monitor Adaptive Server, see the *Unified Agent / Agent Management Console User's Guide*.

Monitoring Servers with the Control Panel

The Control Panel uses the Services option to check the local server's status.

1. Go to **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Check the Status column.
   - If the Status value is Started, the server is running.
   - If the Status value is blank, the server is not running.

CHAPTER 9 Adaptive Server Configurations

Adaptive Server includes default parameter settings that you may need to change, depending on your requirements.

Use the Server Config utility to make any configuration changes.

See also

- *Chapter 4, About Changing Adaptive Server Configurations* on page 11
- *Chapter 12, Localization Support* on page 57

Default Adaptive Server Configuration

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

After installing and testing the default Adaptive Server, change any parameter settings to meet your system's needs and install other optional features.

Default Adaptive Server Parameter Settings

After Adaptive Server installation, Adaptive Server parameter settings are set to default values. You may need to configure these settings to suit your computer and database needs.

Item	Default Value
Name	*AdaptiveServername*
Network support	TCP/IP
Socket number	5000
Named pipes	`\pipe\sybase\server`
Command line options	None
Error log path	`%SYBASE%\%SYBASE_ASE%\install/errorlog`
Event logging	Not configured
Language	us_english
Character set	cp850
Sort order	Binary ordering

Item	Default Value
Login security mode	Standard

Default Backup and XP Server Settings

After Adaptive Server installation, Backup and XP Server settings are set to default values. You may need to configure these settings to suit your computer and database needs.

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	*%SYBASE%\%SYBASE_ASE\install\backup.log*
XP Server	Name	*AdaptiveServername*_XP
	Network support	Named Pipes, Windows Sockets (TCP/IP)
	Pipe name	*\pipe\sybase\xp*
	Socket number	5002
	Error log path	N/A

Change Adaptive Server Configurations

To change configuration settings for Adaptive Server, use the Server Config utility.

You can run Server Config either by:

- Selecting Server Config from within Windows, or by,
- Running **sp_configure** from within **isql.** Use **sp_configure** to quickly and easily change single parameters and values. For more information, see **sp_configure** in the *Reference Manual: Procedures*.

Note: Adaptive Server 15.0.3 and later installers allow you to tune basic configuration settings during installation, instead of as a post installation task. See the *Installation Guide*.

Starting Server Config

Start the Server Config utility from the Windows Start menu. To run this utility from the Windows command prompt, run **syconfig.exe**.

1. Select **Start > Programs > Sybase > Adaptive Server Enterprise > Server Config**.

2. When you complete the necessary configuration changes, click **Exit**.

Configuring Adaptive Server

Use Change Options from within Server Config to configure Adaptive Server.

1. Start Server Config.
2. Click the **Adaptive Server** icon, and click **Configure Adaptive Server** from the Configure Sybase Servers dialog box.
3. Select the name of the server to configure, and click **Continue**.
4. Enter 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.
6. Select the option to configure:
   - Command Line
   - Default Backup Server
   - Default XP Server
   - Two Phase Commit – see the *Adaptive Server Installation Guide* for your platform.
   - Error Log Path
   - Event Logging
   - Language – see the *Adaptive Server Installation Guide* for your platform.
   - Login Security

Setting Adaptive Server Parameters

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

1. Click **Command Line** from the Change Options box on the Configuring Adaptive Server Enterprise dialog box.
2. Enter the parameters and values you want to set for Adaptive Server.

   Enter the parameters as you would at the command line. However, omit the command itself and any parameters that might vary.
3. Click **OK**, then 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.

1. Click **Default Backup Server** from the Change Options buttons.

2. Enter the name of the Backup Server to use as the new default, and click **OK**.
3. Click **Save** then 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 file name. 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 with Sybmail.

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 file name. For example, Backup Server for an Adaptive Server named PIANO is named PIANO_BS.

1. Start Server Config.
2. Click the **Backup Server** icon, then click **Configure Backup Server**.
3. Select the name of the server to configure and click **Continue**.
4. Change the error log path, language, and character set as necessary.

   For more information about languages and character sets, see the *Installation Guide*.
5. Click **Save**, then click **Exit** to quit Server Config.

Configuring Job Scheduler and Self Management

Job Scheduler defines and schedules database administration and maintenance tasks. Self Management is the Adaptive Server ability to monitor and adjust its state as necessary. You can create and schedule jobs for maintenance and tuning tasks to extend the Adaptive Server self-management capabilities.

You can configure Job Scheduler and Self Management only in resource file mode.

In resource file mode, edit the sample resource file `%SYBASE%\%SYBASE_ASE%\sample\server\sybatch_js.res` and execute:

```
sybatch.exe -r sybatch_js.res
```

See the *Job Scheduler Users Guide*.

CHAPTER 10 Network Communications Using sql.ini

Adaptive Server communicates 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. You can configure Adaptive Server to use `sql.ini` file connections.

Use Server Config to change the values that Adaptive Server can access.

Adaptive Server on Windows 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.

Two files control how clients find servers and drivers:

- The `sql.ini` file lists 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.

Client Connections to Adaptive Server

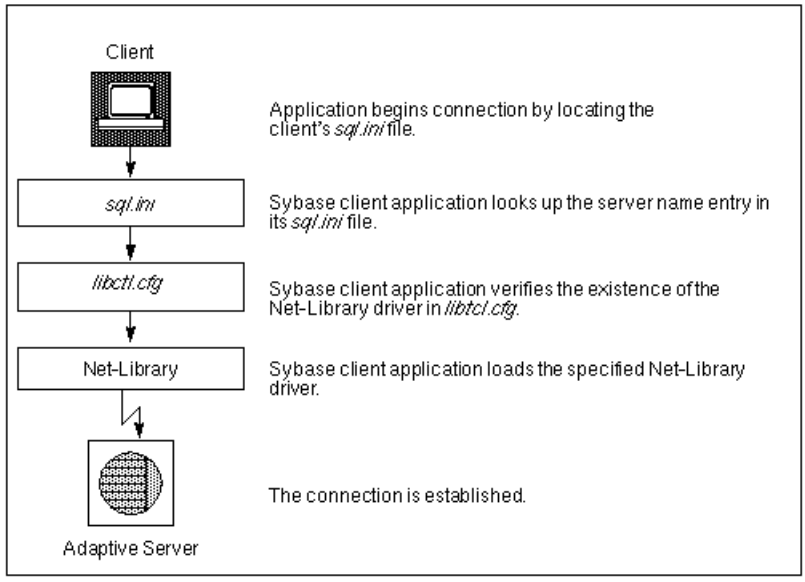
Client software connects to Adaptive Server by looking at the `sql.ini` file and the `libtcl.cfg` file and loading the specified Net-Library driver.

Each client:

1. Determines the name of the Adaptive Server by finding the value of the DSQUERY environment variable.
2. Looks in the `sql.ini` file for an entry that 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 2: Connecting to Adaptive Server



Determine the Address to Listen for Client Connections

Adaptive Server uses the `sql.ini` file to determine the address at which to listen for clients.

Once started, the Adaptive Server:

1. Finds the value of the DSLISTEN environment variable.
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 to listen for client connection requests.

Client Access to Adaptive Server

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

Enabling Client Access to a Server

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

To create a new `sql.ini` file, use the Directory Services Editor utility, **dsedit**.

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 using **dsedit**, see the *Utilities Guide*.

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.

1. Select **Start > Programs > Sybase > Connectivity > Open Client Directory Service Editor**.
2. Select a driver from the DS Name list, and click **OK**.
3. Select **Server Object** menu, and select **Add**.
4. Enter the name of the server to add, and click **OK**.
5. Select the new server name, which you have just added, from the Server list.
6. Enter the server's address:
   a) Select **Server Address** from the Attributes box on the Interfaces Driver window.
   b) Select **Server Object > Modify Attribute**.
   c) Click **Add**.
   d) Choose the appropriate protocol, enter the network address, and click **OK**.
7. Click **OK**.

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

Components in the sql.ini File

The `sql.ini` file includes the server name, network driver, service type, and server address. Understanding these components is useful background information for editing an `sql.ini` file.

The `sql.ini` file looks similar to:

```
[PIANO_XP]
master=NLWNSCK,PIANO,5002
query=NLWNSCK,PIANO,5002


[PIANO]
master=NLWNSCK,PIANO,5000
query=NLWNSCK,PIANO,5000


[PIANO_BS]
master=NLWNSCK,PIANO,5001
query=NLWNSCK,PIANO,5001


[PIANO_JSAGENT]
master=NLWNSCK,PIANO,4900
query=NLWNSCK,PIANO,4900


[ws]
master=NLWNSCK,PIANO,8183
```

Server Name

The server name is the Adaptive Server to which clients connect.

Use these 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 file names.
- Adaptive Server names are not case-sensitive. For example, “PRODUCTION,” “Production,” and “production” are interpreted as the same server name.
- Server names cannot contain multibyte characters.

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 service as either MASTER or 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 for a computer that is running clients only.
- QUERY represents the service that a client application uses to log in to 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

The server address is the address at which Adaptive Server listens for client connections.

The address requires this information:

- Address format
- IP address
- Named Pipes format
- Widows 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 these 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 is connecting.
- Port addresses must be unique to each server. The port address is determined by the port number provided in the `sql.ini` file, and the IP address.
- By default, the port number for Adaptive Server is 5000; for Backup Server, it is 5001.

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\query
```

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

```
NLMSNMP,\\130.214.60.230\pipe\sybase\query
```

Named Pipes Format

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

Use these 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 the following, where *machine_name* is the name of the computer that runs the server:

```
\\machine_name
```

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. Also, 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 Windows computer, and a unique socket for the Adaptive Server, separated by a comma.

Keep these 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. 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 Windows Registry to increase the maximum number of sockets connections available on the server.

Warning! Do not modify a Registry value unless you are an Windows administrator and are familiar with the **regedt32** utility. See your Windows operating system documentation.

Modifying an Existing TcpNumConnections Value

Modify the maximum number of connections that TCP can have open simultaneously.

1. Log in to Windows using an account with Windows administrator privileges, or use the default "sa" login.
2. From the Run prompt, start the **regedt32** utility.
3. Select the Registry window HKEY_LOCAL MACHINE.
4. Open the Registry key HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet \Services\Tcpip\Parameters.
5. If the TcpNumConnections value exists, double-click it.

   If the value does not exist, add and configure it.
6. In the DWORD Editor dialog box, select the **Decimal** option.
7. Enter the maximum number of connections to support.
8. Click **OK** to return to the Registry key dialog box.

9. Select **Exit** from the Registry menu to quit **regedt32**.
10. Restart your computer.

Adding a TcpNumConnections Value

Add a maximum number of connections that TCP can have open simultaneously.

1. Complete the Add Value dialog box:
   - Value Name – select **TcpNumConnections**.
   - Data Type – select **REG_DWORD**.
2. Click **OK**.
3. Complete the DWORD Editor dialog box:
   - Data – enter the maximum number of TCP connections for the computer.
   - Radix – select **Decimal**.
4. Click **OK**.

   The utility adds the new value to the Registry key.
5. Choose **Exit** from the Registry menu to quit **regedt32**.
6. Restart your computer.

Using Multiple TCP/IP Network Interface Cards

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

When entering 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
master=NT2,5000
```

Controlling the Connection Timeout

To avoid a connection error, increase the TcpKeepTries value.

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 Windows TcpKeepTries. To correct this problem, increase the value.

Warning! Do not modify Registry values unless you are an Windows Administrator and you are familiar with the **regedt32** utility. See the Windows operating system documentation.

Increasing the TcpKeepTries Value

Increase the maximum number of attempts before the connection times out.

1. Start the **regedt32** utility, and display the Parameters values.
2. Double-click the TcpKeepTries value.
3. Change the data value to at least 20, and then click **OK**.
4. Choose **Exit** from the Registry menu to quit.
5. Restart 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 Windows operating system. 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

Some NWLink IPX/SPX connection formats are acceptable for the MASTER entry, some formats are unacceptable for accessing a local Adaptive Server, and only Format 1 and Format 3 are acceptable for QUERY entries.

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

The *net_number* is the network number that you specified during the NWLink IPX/SPX configuration.

To find the network number:

1. In the Window's Control Panel, open Network and Dial-up Connections.
2. Right-click **Local Area Connection**, then click **Properties**.
3. Double-click **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol**.
4. The current network number is the decimal number that appears in the "Internal network number" field.

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

```
net config workstation
```

```
Computer name                \\PIANO
User name                    user1
Workstation active on        NBT_Elnk31 (00A0242EA892)
Software version             Windows 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.

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

Share Network Configuration Information

You can share identical network information across multiple systems by either creating a master interface (`sql.ini`) file or by using Windows 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, and you can use it 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.

To maintain consistency in the `sql.ini` files on a network, make the changes to one version of the file, then copy that file to the rest of the computers on the network. For this task, you can use Windows File Replication to copy the file to many computers.

Windows Registry as a Directory Service

Before using the Windows Registry as a directory service, review your Sybase products.

- 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 creating and maintaining 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 must maintain a `sql.ini` file if users are to connect from any of the Sybase client applications, such as Sybase Central.

Using Windows Registry as a Directory Service

Create server name keys under the Registry key specified for "ditbase" in `libtcl.cfg`.

Prerequisites

Access both the Open Client/Open Server Configuration and the **dsedit** utilities.

Task

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

1. Make sure the `ocscfg.dat` file is in your `d:\sybase\OCS-15_0\bin` directory.
2. Start the OC OS Config Utility.
   a) Select **Start > Programs > Sybase > Connectivity > Open Client Directory Service Editor**.
   b) Select the **Directory Services** tab

c) Click **Add**
d) Enter REGISTRY for the DS Name.
e) Enter LIBDREG for the Directory Service Driver or select it from the drop-down list.
f) Enter *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**.

Alternatively, you can use a text editor to add these 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 **Start > Programs > Sybase > Connectivity > Open Client Directory Service Editor**.
   b) Registry from the DS Name list, and click **OK**.
   c) Create server entries using **dsedit**.

Verify 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.

Use **dsedit** to test connections.

Configure 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, PowerDesigner™ connects through the ODBC driver. Other third-party applications may also require the ODBC driver.

For Adaptive Server versions earlier than 12.5, ODBC connections are built on top of the Open Client Client-Library, so you must install the Open Client software on the clients where you install the ODBC Driver.

You can also install the driver separately on other client workstations on which you run third-party or developed products.

See the *ODBC Driver Reference Guide*.

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

Configuring the ODBC Driver

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

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

   For more information about ODBC, see your Windows operating system documentation.
2. Click the **System DSN** tab.
3. Click **Add**.
4. Select **Adaptive Server ODBC Driver** as the driver to use for Adaptive Server, then click **Finish**.
5. Complete the ODBC Adaptive Server Setup dialog box:
   - Data Source Name – enter a short description of the Adaptive Server. 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) – a long description of a data source name; for example, "Accounting database on Adaptive Server 3."
6. Click the **Options** button.
7. Enter the name of the database to which to connect:

   For a PowerDesigner connection, you need not specify a database unless you want to reverse-engineer it. In this case, "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*.
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.

IPv6 Support

Adaptive Server supports IPv6 technology.

IPv6 addressing terminology:

- Link-local address – an IPv6 address that is usable only over a single link.
- Site-local address – an IPv6 address that can be used within a single site.
- Global address – an IPv6 address that can be used across the Internet.

Note: Interfaces files also provide IPv6 support.

IPv6 application types:

- IPv6-unaware – an application that cannot handle IPv6 addresses.
- IPv6-aware – an application that can communicate with nodes that do not have IPv4 addresses. In some cases, this might be transparent to the application, for instance if the API hides the content and format of actual addresses.
- IPv6-enabled – an application that, in addition to being IPv6-aware, takes advantage of some IPv6 features.
- IPv6-required – an application that requires some IPv6 features and cannot operate over IPv4.

IPv6 Infrastructure

Use Adaptive Server as an IPv6-aware server only in a dual-stack infrastructure, which implements both IPv4 and IPv6.

Sybase applications are IPv6-aware, using the IETF designed primitives.

Table 2. IPv6 Support

Platform	Adaptive Server IPv6 Awareness	Open Client/Server IPv6 Awareness
Sun Solaris 8 32- and 64- bit	12.5.3a and 15.0	12.5 and 15.0
HP-UX 11i(v1) 32- and 64-bit	12.5.3a and 15.0	12.5 and 15.0
Microsoft Server 2003	12.5.3a and 15.0	12.5 and 15.0
Linux RHEL 3.0	15.0	12.5 and 15.0

Many Sybase products that are Open Client/Server-based, like XP Server, Backup Server, Replication Server and Open Switch became automatically IPv6-aware due to the layered Open Client Transport Control Layer (CTlib->NETlib) which is IPv6-aware for network-socket operations. DBlib-based Open Client products are not IPv6-aware.

Some third-party components in Adaptive Server are not yet IPv6-aware. The functional mechanisms of Adaptive Server Enterprise that are IPv6-aware with respect to the platform / release matrix include:

- Connection handler
- RPC mechanisms
- Job Scheduler Task / agent session connection
- Network host API
- UDP message support for `sybsendmsg`
- Component Integration Services connectivity
- Host / name resolving
- XML URL connection handler
- Auditing for client address data

The following functional mechanisms in Adaptive Server Enterprise do not currently support IPv6:

- Java support
- License Management Server
- LDAP driver

Before starting Adaptive Server for IPv6-aware operations, make sure that your infrastructure is correctly set up. Once your operating system is correctly configured, you can configure and enable an IPv6 connection handler. Configuring and enabling the IPv6 connection handler requires an additional DCL entry. A single Adaptive Server configuration can typically carry up to 32 connection handler assignments within the DCL.

For example if you have a site-local setup with two domains administrated under the name server setup:

```
sybase.com - being responsible for all IPv4 networking applications
v6.sybase.com - being responsible for all IPv6 networking
applications
```

The DCL entry for Adaptive Server named “SYBASE” on the host “revival” for port 17100 should look similar to:

```
SYBASE
master tcp ether revival.sybase.com 17100
query tcp ether revival.sybase.com 17100
master tcp ether revival.v6.sybase.com 17100
query tcp ether revival.v6.sybase.com 17100
```

When Adaptive Server is started with IPv6-awareness, it creates two connection handlers. One listens on port 17100 for incoming IPv4 clients connection requests, and the other listens on port 17100 for incoming IPv6 clients connection requests.

Note: When you start Adaptive Server, you can set Trace flag 7815 to capture and log IPv4 and IPv6 client address connection requests and host / name lookups.

CHAPTER 11 Lightweight Directory Access Protocol in Adaptive Server

Lightweight Directory Access Protocol (LDAP) is an industry standard for accessing directory services. Directory services allow components to look up information by a distinguished name (DN) from an LDAP server that stores and manages server, user, and software information that is used throughout the enterprise or over a network.

The LDAP server can be located on a different platform from the one on which Adaptive Server or the clients are running. LDAP defines the communication protocol and the contents of messages exchanged between clients and servers. Messages are operators, such as client requests for read, write and query, and server responses, including data-format information.

The LDAP server stores and retrieves information about:

- Adaptive Server, such as IP address, port number, and network protocol
- Security mechanisms and filters
- High availability companion server name

You can configure an LDAP server with these access restrictions:

- Anonymous authentication – all data is visible to any user.
- User name and password authentication – Adaptive Server uses the default user name and password from Windows – `%SYBASE%\%SYBASE_OCS%\ini\libtcl.cfg`.

User name and password authentication properties establish and end a session connection to an LDAP server.

Note: The user name and password that are passed to the LDAP server for user authentication purposes are distinct and different from those used to access Adaptive Server.

When an LDAP server is specified in the `libtcl.cfg` file, the server information is accessible only from the LDAP server. Adaptive Server ignores the interfaces file.

If multiple directory services are supported in a server, then the order in which they are searched is specified in `libtcl.cfg`. You cannot specify the search order with the `dataserver` command line option.

LDAP Directory Services versus the Sybase Interfaces File

The LDAP driver implements directory services for use with an LDAP server.

LDAP directories provide:

- A network-based alternative to the traditional Sybase interfaces file
- A single, hierarchical view of information, including users, software, resources, networks, files, and so on

Interfaces File	Directory Services
Platform-specific	Platform-independent
Specific to each Sybase installation	Centralized and hierarchical
Contains separate master and query entries	One entry for each server that is accessed by both clients and servers
Cannot store metadata about the server	Stores metadata about the server

LDAP directory services support more attributes than the Sybase interfaces file. These attributes can include server version, server status, and so on.

Note: LDAP is supported only with reentrant libraries. When you are connecting to a server using LDAP directory services, you must use **isql_r**, instead of **isql**.

Table 3. Sybase LDAP Directory Definitions

Attribute Name	Value Type	Description
ditbase	`interfaces` file or `libtcl.cfg`	DIT base for object tree. If the `libtcl.cfg` file is specified, the `interfaces` file is ignored. You can use **ct_con_prop()** to override the `libtcl.cfg` file for a specified connection.
dn	Character string	Distinguished name. Must be a unique name that identifies the object.
sybaseVersion	Integer	Server version number.
sybaseServername	Character string	Server name.
sybaseService	Character string	Service type: Sybase Adaptive Server, or Sybase SQL Server.
sybaseStatus	Integer	Status: 1 = Active, 2 = Stopped, 3 = Failed, 4 = Unknown.

Attribute Name	Value Type	Description
sybaseAddress	String	Each server address includes: • Protocol: TCP, NAMEPIPE, SPX DECNET (entry is case-sensitive). • Address: any valid address for the protocol type. `dscp` splits this attribute into Transport type and Transport address.
sybaseSecurity (optional)	String	Security OID (object ID).
sybaseRetryCount	Integer	This attribute is mapped to CS_RETRY_COUNT, which specifies the number of times that **ct_connect** retries the sequence of network addresses associated with a server name.
sybaseRetryDelay	Integer	This attribute is mapped to CS_LOOP_DELAY, which specifies the delay, in seconds, that **ct_connect** waits before retrying the entire sequence of addresses.
sybaseHAservername (optional)	String	A secondary server for failover protection.

The traditional interfaces file with TCP connection and a failover machine looks like:

```
master tcp ether huey 5000
query tcp ether huey 5000
hafailover secondary
```

An example of an LDAP entry with TCP and a failover machine looks like:

```
dn: sybaseServername=foobar, dc=sybase,dc=com
objectClass: sybaseServer
sybaseVersion: 1500
sybaseServername: foobar
sybaseService: ASE
sybaseStatus: 4
sybaseAddress: TCP#1#foobar 5000
sybaseRetryCount: 12
sybaseRetryDelay: 30
sybaseHAServernam: secondary
```

All entries in the LDAP directory service are called entities. Each entity has a distinguished name (DN) and is stored in a hierarchical tree structure based on its DN. This tree is call the *directory information tree* (DIT). Client applications use a DIT base to specify where entities are stored.

In the example above, the entry describes an Adaptive Server named “foobar” listening on a TCP connection with a port number of 5000. This entity also specifies a retry count of 12

(times) and a retry delay of 30 (seconds). Once a client has found an address where a server responds, the login dialog between the client and the server begins.

You can find a complete list of the Sybase LDAP directory schema in `%SYBASE%\%SYBASE_OCS%\ini`. In the same directory, there is also a file called `sybase-schema.conf`, which contains the same schema, but uses a Netscape-specific syntax.

Since LDAP supports multiple entries for each attribute, each address attribute must contain the address of a single server, including protocol, access type, and address.

For example, this is an LDAP entry for an Windows server listening on two addresses, with different connection protocols:

```
sybaseAddress = TCP#1#TOEJAM 4444
sybaseAddress = NAMEPIPE#1#\pipe\sybase\query
```

Note: Each entry in the address field is separated by the # character.

You can edit these entries with **dsedit**.

To ensure cross-platform compatibility for all Sybase products, the protocol and address attribute fields should be in a platform- and product-independent format.

The libtcl.cfg File

Use the `libtcl.cfg` file to specify the LDAP server name, port number, DIT base, user name, and password to authenticate the connection to an LDAP server.

The purpose of the `libtcl.cfg` file is to provide configuration information such as driver, directory, and security services for Open Client/Open Server and Open Client/Open Server-based applications. 32-bit utilities, such as **dsedit** and **srvbuild**, look up the `libtcl.cfg`.

The default `libtcl.cfg` file is located in `%SYBASE%\%SYBASE_OCS%\ini`.

If LDAP is specified in the `libtcl.cfg` file, the interfaces file is not used.

Note: Open Client/Open Server applications that use the `-I` option at start-up override the `libtcl.cfg` file and use the interfaces file.

In its simplest form, the `libtcl.cfg` file is in this format:

```
[DIRECTORY]
```

```
ldap=libsybdldap.dll  ldapurl
```

where the *ldapurl* is defined as:

```
ldap://host:port/ditbase
```

The following LDAP entry, using these same attributes, is an anonymous connection and works only if the LDAP server allows read-only access.

```
ldap=libsybdldap.dll ldap://ldaphost/d=sybase,dc=com
```

To enable password authentication at connection time, you can specify a user name and password in the `libtcl.cfg` file as extensions to the LDAP URL.

Enabling LDAP Directory Services

To use a directory service, you must enable LDAP Directory Services.

1. Configure the LDAP server according to the vendor-supplied documentation.
2. Add the location of the LDAP libraries to the PATH environment variable for your platform.
3. Configure the `libtcl.cfg` file to use directory services.

   Use any standard ASCII text editor to:

   - Remove the semicolon (;) comment markers from the beginning of the LDAP URL lines in the `libtcl.cfg` file under the `[DIRECTORY]` entry.
   - Add the LDAP URL under the `[DIRECTORY]` entry.

   Warning! The LDAP URL must be on a single line.

   ```
   ldap=libsybdldap.dll
   ldap://ldaphost/dc=sybase,dc=com??one??
   bindname=uid=Manager,dc=sybase,
   dc=com?password
   ```

   For example:

   ```
   [DIRECTORY]
   ldap=libsybdldap.dll ldap://ldaphost/dc=sybase,dc=com??one??
   bindname=uid=Manager,dc=sybase,
   dc=com?password
   ```

   "*one*" indicates the scope of a search that retrieves entries one level below the DIT base.

Table 4. ldapurl Variables

Keyword	Description	Default
host (required)	The host name or IP address of the machine running the LDAP server	None
port	The port number that the LDAP server is listening on	389
ditbase (required)	The default DIT base	None
username	Distinguished name (DN) of the user to authenticate	NULL (anonymous authentication)

Keyword	Description	Default
password	Password of the user to be authenticated	NULL (anonymous authentication)

4. Verify that the appropriate environment variable points to the required third-party libraries. The Netscape LDAP SDK libraries are located in `%SYBASE%\%SYBASE_OCS\lib3p`.The Windows PATH environment variable must point to this directory.
5. Use **dscp** or **dsedit** to add your server entry to the LDAP server.

Adding a Server to the Directory Services

Each server entry is made up of a set of attributes. When you add or modify a server entry, you are prompted for information about server attributes.

Some attributes are provided by default, others require user input. When a default value is provided, it appears in brackets "[ ]".

Warning! Most LDAP servers have an **ldapadd** utility for adding directory entries. Sybase recommends you use **dsedit** instead since it has built-in semantic checks that generic tools do not provide.

You can use **srvbuild** to add entries, but not modify or delete them.

Adding a Server Entry to the Directory Service Using dsedit

Use **dsedit** to add a server to the directory service.

Prerequisites

Add the LDAP URL to the `libtcl.cfg` file.

Task

1. In Windows, select **Start > Programs > Sybase > Connectivity > Open Client Directory Service Editor**.
2. Select LDAP from the list of servers, and click **OK**.
3. Click **Add New Server Entry**.
4. Enter:
   - The server name – required.
   - Security mechanism – optional. A list of security mechanism OIDs are located in `%SYBASE%\ini\objectid.dat`.
   - HA server name – optional. This is the name of the high-availability failover server, if you have one.

5. Click **Add New Network Transpor**t.
   - Select the transport type.
   - Enter the host name.
   - Enter the port number.
6. Click OK twice to exit the **dsedit** utility.

To view the server entries, enter this URL in Netscape:

```
ldap://host:port/ditbase??one
```

For example:

```
ldap://huey:11389/dc=sybase,dc=com??one
```

Note: Microsoft Internet Explorer does not recognize LDAP URLs.

For more information about `dscp`, see the *Open Client/Server Configuration Guide*.

Multiple Directory Services

Any type of LDAP service, whether it is an actual server or a gateway to other LDAP services, is called an LDAP server. You can specify multiple directory services for high-availability failover protection.

Not every directory service in the list must be an LDAP server.

For example:

```
[DIRECTORY]

ldap=libsybdladp.so ldap://test:389/dc=sybase,dc=com
ldap=libsybdldap.so ldap://huey:11389/dc=sybase,dc=com
```

In this example, if the connection to *test:389* fails, the connection fails over to the DCE driver with the specified DIT base. If this also fails, a connection to the LDAP server on *huey:11389* is attempted. Different vendors employ different DIT base formats.

Note: For more information, see the *Open Client Client-Library/C Programmer Guide* and the *Open Client Client-Library/C Reference Manual*

Encrypting the Password

Entries in the `libtcl.cfg` file are in human-readable format. Sybase provides a **pwdcrypt** utility for basic password encryption. **pwdcrypt** is a simple algorithm that, when applied to keyboard input, generates an encrypted value that can be substituted for the password. **pwdcrypt** is located in `%SYBASE%\%SYBASE_OCS%\bin`.

From the `%SYBASE%\%SYBASE_OCS%` directory, enter:

```
bin/pwdcrypt
```

Enter your password twice when prompted.

pwdcrypt generates an encrypted password. For example:

```
0x01312a775ab9d5c71f99f05f7712d2cded2i8d0ae1ce78868d0e8669313d1bc4c
706
```

Copy and paste the encrypted password into the `libtcl.cfg` file using any standard ASCII-text editor. Before encryption, the file entry appears as:

```
ldap=libsybdldap.dll
ldap://ldaphost/dc=sybase,dc=com??one??
bindname=uid=Manager,dc=sybase,
dc=com?password
```

Replace the password with the encrypted string:

```
ldap=libsybdldap.dll
ldap://ldaphost/dc=sybase,dc=com??one??
bindname=uid=Manager,dc=sybase,dc=com?
0x01312a775ab9d5c71f99f05f7712d2cded2i8d0ae1ce78868d0e8669313d1bc4c
706
```

Warning! Even if your password is encrypted, you should still protect it using file-system security.

Performance with LDAP

Performance when using an LDAP server may be slower than when using an interfaces file because the LDAP server requires time to make a network connection and retrieve data.

Since this connection is made when Adaptive Server is started, performance changes are seen at login time, if at all. During normal system load, the delay should not be noticeable. During high system load with many connections, especially repeated connections with short duration, the overall performance difference of using an LDAP server versus the traditional interfaces file might be noticeable.

Migrating from the sql.ini File to LDAP

Before you can configure your server to use LDAP service, you must upgrade the server.

There is no direct method to upgrade an existing server using the `sql.ini` file to one that uses LDAP. To upgrade, see the *Installation Guide for Windows*.

If you have LDAP or other directory services defined in the `libtcl.cfg` file before configuring the server, the `-i` argument is not added to the `sql.ini` file.

If you do not have LDAP or other directory services defined in the `libtcl.cfg`, the `-i` argument is added to the Windows Registry for your SYBASE server.

1. Shut down the server.
2. Edit the `%SYBASE%\%SYBASE_OCS%\ini\libtcl.cfg` file to add the directory service.
3. Use **dsedit** and add the server entry to directory service.
4. Start the configuration utility. Select**Start** > **Programs** > **Sybase** > **Sybase** > **Server Config**.
5. Select **Configure Adaptive Server**.
6. Select the server for which to enable directory service, and click **Continue**.
7. Enter your login name and password, and click **Continue**.
8. When prompted to start the server, select **Yes**.
9. On the Configure Adaptive Server screen, click **Cancel** or **Save**.
10. Exit Server Config.

Alternatively, you can add or remove the `-i` argument which specifies the interfaces (`sql.ini` on Windows) file directly from the Windows registry.

1. Select **Start** > **Run** and enter, regedt32.
2. Select the HKEY_LOCAL_MACHINE view.
3. Select SOFTWARE\Sybase\Server\`server_ name`\Parameters
4. Remove the `-i` argument from the line that ends with ...`\Sybase\ini\sql.ini`

CHAPTER 12 Localization Support

Localization is setting up an application to run in a particular language or country environment, including translated system messages and correct formats for date, time, and currency. Adaptive Server supports localization for international customers and for customers with heterogeneous environments.

Localization support includes:

- Data processing support – Adaptive Server comes with character set and sort-order definition files it uses or processing the characters used in different languages.
  Sybase provides support for the major languages in:
  - Western Europe
  - Eastern Europe
  - Middle East
  - Latin America
  - Asia
- Translated system messages – Adaptive Server includes language modules for:
  - Brazilian Portuguese
  - Chinese (Simplified)
  - French
  - German
  - Japanese
  - Korean
  - Polish
  - Spanish
  - Thai
- Translated documentation – translated documentation is available in:
  - Chinese (Simplified)
  - French
  - German
  - Japanese
  - Korean
  - Polish
  - Spanish

See also

- *Chapter 4, About Changing Adaptive Server Configurations* on page 11
- *Chapter 9, Adaptive Server Configurations* on page 27

Language Modules

Adaptive Server stores its localized software messages in separate language modules.

When you install a language module, the installation program loads the messages, character set, and sort-order files that support the new language in the correct locations.

By default, Adaptive Server and Backup Server installs English system messages in English are installed by defaut.

Default Character Sets for Servers

The default character set is the character set in which data is encoded and stored on the Adaptive Server databases.

By default, Adaptive Server and Backup Server on Windows systems install the character set files for CP 850, which supports the Western European languages.

Changing the Default Character Set for Servers

You can select any character set as the default on Adaptive Server, including character sets that are not the platform default character sets.

Keep these guidelines in mind when selecting a new default character set:

- To avoid conversion errors or overhead, determine the default character set based on the character set used by your clients.

  For example, if most of your clients use ISO 8859-1, you can minimize the amount of data conversion by specifying ISO 8859-1.
- If your server is operating in a heterogeneous environment, choose a character set that works with all the character sets needed. Often, this is Unicode (UTF-8).

Warning! Make all changes to the default character set and sort order for a new Adaptive Server before creating any user databases or making any changes to the Sybase-supplied databases. Changing the character set and sort order after data or data structures have been added to Adaptive Server can cause incorrect behavior. To change the character set or sort order after you have added data, see the *System Administration Guide: Volume 1.*

Supported Character Sets

Adaptive Server supports many languages, scripts and character sets.

Arabic Character Sets

Adaptive Server supports Arabic character sets.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
cp864	X	PC Arabic
cp1256	X	Microsoft Windows Arabic
iso88596	X	ISO 8859-6 Latin/Arabic

Baltic Character Set

Adaptive Server supports the Baltic character set.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
cp1257	X	Microsoft Windows Baltic

Simplified Chinese Character Sets

Adaptive Server supports Simplified Chinese character sets.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
eucgb	X	EUC GB encoding = Simplified Chinese character sets
cp936	X	Microsoft Simplified Chinese character sets
gb18030	X	RC 18030 standard

Traditional Chinese Character Set

Adaptive Server supports Traditional Chinese character sets.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
cp950	X	PC (Microsoft) Traditional Chinese
euccns	X	EUC CNS encoding = Traditional Chinese with extensions
big5	X	Big 5 Traditional Chinese
big5hk	X	Big 5 with HKSCS extensions

Cyrillic Character Sets

Adaptive Server supports Cyrillic character sets.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
cp855		IBM PC Cyrillic
cp866		PC Russian
cp1251		Microsoft Windows 3.1 Cyrillic
iso88595		ISO 8859-5 Latin/Cyrillic
koi8		KOI-8 Cyrillic
mac_cyr		Macintosh Cyrillic
kz1048		Kazakhstan Cyrillic

Eastern European Character Sets

Adaptive Server supports Eastern European character sets.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
cp852		PC Eastern Europe
cp1250		Microsoft Windows 3.1 Eastern European
iso88592		ISO 8859-2 Latin-2
mac_ee		Macintosh Eastern European

Greek Character Sets

Adaptive Server supports Greek character sets.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
cp869		IBM PC Greek
cp1253		MS Windows Greek
greek8		HP GREEK8
iso88597		ISO 8859-7 Latin/Greek
macgrk2		Macintosh Greek

Hebrew Character Sets

Adaptive Server supports Hebrew character sets.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
cp1255	X	Microsoft Windows Hebrew
iso88598	X	ISO 8859-8 Hebrew

Japanese Character Sets

Adaptive Server supports Japanese character sets.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
cp932	X	IBM J-DBCS:CP897 + CP301 (Shift-JIS)
deckanji		Digital UNIX JIS encoding
eucjis		EUC-JIS encoding
sjis		Shift-JIS (no extensions)

Korean Character Set

Adaptive Server supports the Korean character set.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
eucksc	X	EUC KSC Korean encoding = CP949

Thai Character Sets

Adaptive Server supports Thai character sets.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
tis620	X	TIS-620 Thai standard
cp874	X	Microsoft Windows Thai

Turkish Character Sets

Adaptive Server supports Turkish character sets.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
cp857		IBM PC Turkish
cp1254		Microsoft Windows Turkish
iso88599		ISO 8859-9 Latin-5 Turkish
macturk		Macintosh Turkish
turkish8		HP TURKISH8

Unicode Character Set

Adaptive Server supports the Unicode character set (which supports over 650 languages).

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
utf8	X	Unicode UTF-8 encoding

Vietnamese Character Set

Adaptive Server supports Vietnamese character sets.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
cp1258	X	Microsoft Windows Vietnamese

Western European Character Sets

Adaptive Server supports Western European character sets.

- X – requires Unilib® conversion.
- No X – may use either the Unilib conversion or the built-in conversion.

Character Set	Unilib Required	Description
ascii8	X	US ASCII, with 8-bit data, ISO 646
cp437		IBM CP437 – US code set
cp850		IBM CP850 – European code set
cp860	X	PC Portuguese
cp863	X	IBM PC Canadian French code page
cp1252	X	Microsoft Windows US (ANSI)
iso_1		ISO 8859-1 Latin-1
mac		Standard Macintosh coding
roman8		HP ROMAN8
iso 885915	X	ISO 8859-15 Latin-1 with Euro support

Character Set Conversion

Backup Server passes messages to Adaptive Server in the client's language and in the Adaptive Server character set. Adaptive Server converts the messages and issues them in the client's language and character set.

Keep these requirements in mind when selecting a character set:

- In a heterogeneous environment, Adaptive Server and Backup Server may need to communicate with clients running on different platforms and using different character sets. To maintain data integrity, the server converts the code between the character sets.
- To use the built-in conversion, install the character set definition files on the server for all the character sets being used by your clients. Built-in conversion support is available for many character sets.
- Unilib conversion support is available for all character sets supported by Sybase. To enable Unilib conversion, you must use **sp_configure** and turn **enable unicode conversions** on. See the *System Administration Guide: Volume 1*.

If either Adaptive Server or Backup Server does not support a client's language or character set, the server issues a warning message. Errors also occur when the Backup Server character set is incompatible with the Adaptive Server character set. By default, Unicode conversion is enabled.

Character set conversion is supported only between character sets for the same language or between character sets in the same language group.

For example, automatic character set conversion is supported between the character sets for the Western European languages: ASCII 8, CP 437, CP 850, CP 860, CP 863, CP 1252, ISO 8859-1, ISO 8859-15, and ROMAN8. Similarly, conversion is supported between the character sets for Japanese: CP 932, EUC-JIS, Shift-JIS, and DEC-Kanji.

However, code conversion is not supported between any of the Western European language character sets and the Japanese character sets. For more information about supported conversions, see the *System Administration Guide: Volume 1*.

Conversions Between Server and Client

If Adaptive Server does not support the client's language or character set, the client can connect with the server, but no character conversions occur.

When a localized client application connects to Adaptive Server, the server checks to see if it supports the client's language and character set.

- If Adaptive Server supports the language, it automatically performs all character set conversions and displays its messages in the client's language and character set.
- If Adaptive Server does not support the language, it uses the user's default language or Adaptive Server default language.
- If Adaptive Server does not support the character set, it issues a warning to the client, turns conversion off, and sets the language to US English.

Sort Orders

Each character set comes with one or more sort orders (collating sequences), which are located in the sort-order definition files (`.srt` files). These files accompany the character set definition files and can be found in the same directory.

You can select a sort order for your data according to the needs at your site. The server can support only one sort order at a time, so select one that works for all of your clients.

Warning! Make all changes to the default character set and sort order for a new Adaptive Server before creating any user databases or making any changes to the Sybase-supplied databases. Changing the character set and sort order after data or data structures have been added to Adaptive Server may cause incorrect behavior. To change the character set or sort order after you have added data, see the *System Administration Guide: Volume 1*.

Available Sort Orders

Available sort orders vary according to the character set installed on Adaptive Server.

You can see the available sort orders for your character set by looking in the `.srt` file for your language. Sort orders are stored in:

`%SYBASE%\charsets\`*`<charset_name>`*`\*.srt`

You can specify sort orders during installation, or later, time using the **syconfig** utility.

Sort Order Name	Description
Binary order	Sorts all data according to numeric byte values for that character set. Binary order sorts all ASCII uppercase letters before lowercase letters. Accented or ideographic (multibyte) characters sort in their respective standards order, which may be arbitrary. All character sets have binary order as the default. If binary order does not meet your needs, specify one of the other sort orders during installation, or by using the **syconfig** utility.
Dictionary order, case-sensitive, accent-sensitive	Sorts each uppercase letter before its lowercase counterpart, including accented characters. Recognizes the various accented forms of a letter and sorts them after the associated unaccented letter.
Dictionary order, case- insensitive, accent-sensitive	Uppercase letters are equivalent to their lowercase counterparts and are intermingled in sorting results.
Dictionary order, case-insensitive, accent-insensitive	Case-insensitive dictionary sort order. Diacritical marks are ignored.

Sort Order Name	Description
Dictionary order, case- insensitive with preference	Case preference for collating purposes. A word written with uppercase letters is equivalent to the same word written with lowercase letters. Uppercase and lowercase letters are distinguished only when you use an **order by** clause, which sorts uppercase letters before it sorts lowercase. Do not select this sort order unless your installation requires that uppercase letters be sorted before lowercase letters in otherwise equivalent strings for **order by** clauses. Using this sort order may reduce performance in large tables when the columns specified in an **order by** clause match the key of the table's clustered index.
Alternate dictionary order, case-sensitive	Lowercase variants sorted before uppercase. Use with several of the Western European languages.
Alternate dictionary order, case-insensitive, accent-insensitive	Use with several of the Western European languages.
Alternate dictionary order, case-insensitive, uppercase preference	Use with several of the Western European languages.
Spanish dictionary order, case-sensitive	Use with Spanish and for most Latin American locales.
Spanish dictionary order, case-insensitive	Use with Spanish and for most Latin American locales.
Spanish dictionary order case-insensitive, accent-insensitive	Use with Spanish and for most Latin American locales.
Scandinavian dictionary order, case-sensitive	Use with Scandinavian languages.
Scandinavian dictionary order, case-insensitive, uppercase preference	Use with Scandinavian languages.

Use Server Config to display the sort orders for the character sets you plan to use.

See also

- *charset Utility* on page 77
- *Sybase Character Set Names* on page 75
- *Configuring Adaptive Server for Other Character Sets* on page 72

Language Modules

If you want Adaptive Server error messages to display in a language other than U.S. English (us_english), you must install the appropriate language module.

When you install a new language module, installation automatically loads the language into the Sybase installation directory to support the new language.

Installing a New Language Module

A full installation of Adaptive Server installs all the language components automatically. If you did not select a full installation, manually install additional language modules as required.

1. Load the language module software from the distribution media. You must load this software into the same directory in which you loaded Adaptive Server.
2. Reconfigure the language and, if necessary, the character set and sort order for Adaptive Server.

Message Languages

By default, US English is installed as the language for messages in Adaptive Server.

These rules apply to language modules:

- During Adaptive Server installation or reconfiguration, you can specify a default language other than US English. Make sure you have also installed the language module for the language you specify.
- If your clients require Adaptive Server messages in a language other than US English, you must load the language module for those languages. You can then configure Adaptive Server to the language used by your clients.
- If Adaptive Server does not support messages in a client's language, these clients receive messages in the server default language.

  For example, if your client's language is Latin, the Spanish language module is installed, and if Spanish is specified as the Adaptive Server default language, the client receives messages in Spanish.

Localization

By default, the Adaptive Server and Backup Server configurations use the English locale settings.

English locale settings include:

- Character set definition files for Western European character sets

- Sort-order definition files for Western European character sets
- U.S. English system message files

During the installation process or through reconfiguration, you can specify a different language, character set, and sort order.

Localization Directories

Sybase localization configuration involves the `locales` and `charsets` directories.

The table illustrates the structure of the localization files. It does not show a complete list of all the files.

%SYBASE%/ or $SYBASE/	charsets	charset_name	*.srt files
		charset_name...	charset.loc
		unicode	*.uct files
	locales	language_name	charset_name
		language_name...	charset_name...
		locales.dat	
		message	language_name
			lan- guage_name...

charsets and locales Directories

The %SYBASE%\locales directory contains a subdirectory for each available language. Each language subdirectory contains a subdirectory for each character set available with that language. The files in %SYBASE%\charsets\charset_name contain information related to each particular character set, such as the definition of the character set and any sort orders available for that character set.

- The `.loc` files in these subdirectories enable Adaptive Server or Backup Server to report errors in a specific language, encoded in a specific character set.
  There are a variety of `.loc` files in each subdirectory. Most of these files contain translated error messages for a specific product or utility.
- The `common.loc` file in the `utf8` subdirectory for each language contains localized information, such as local date, time, and currency formatting, that is used by all products.
- The `locales.dat` file contains entries that associate platform-specific locale names with Sybase language and character set combinations.

You can edit the `locales.dat` file to change the default language or character set for a platform, or add new associations between platform locale names and Sybase language and character name sets.

Format of locales.dat File Entries

Each entry in the `locales.dat` file links a platform-specific locale definition to a Sybase language and character set combination.

Each entry uses this format:

```
locale = platform_locale, syb_language, syb_charset
```

where:

- *platform_locale* is the platform-specific keyword for a locale. For acceptable values, see your operating system documentation.

  For the site default locale, *platform_locale* is "default".
- *syb_language* is the language directory to be used from within %SYBASE%`\locales\language_name`.
- *syb_charset* is the character set that determines the character set conversion method and identifies the directory location of the message files for clients from within %SYBASE%`\locales\language_name\charset_name`.

For example, this entry specifies that the default locale uses us_english for the language and iso_1 for the character set:

```
locale = default, us_english, iso_1
```

Client Application Use of locales.dat

Client applications use the `locales.dat` file to identify the language and character set.

The connection process follows these steps:

1. When a client application starts, it checks the operating system locale setting and the `locales.date` file to see if the setting is appropriate for Adaptive Server. For example, a locale entry for French may look like::

   ```
   locale = fr_FR, french, iso_1
   ```
2. When the client connects to Adaptive Server, the language and character set information is passed to Adaptive Server in the login record.
3. Adaptive Server then uses:
   - The character set information, for example, iso_1, to identify the client's character set and verify whether it can convert character data to this character set
   - The language (in the preceding example, French) and character set information to see if it has messages in the client's language

Note: Adaptive Server software comes with some locale entries already defined in the `locales.dat` file. If these entries do not meet your needs, you can either modify them or add new locale entries.

Editing the locales.dat File

Make a copy of the original `locales.dat` file whenever you edit the file, in case you have problems with the resulting edited version.

1. Using a text editor, such as Notepad, open the `locales.dat` file copy.
2. Find the section for Windows, which is enclosed in brackets `[NT]`.
3. Make sure the section contains an entry for the language (*syb_language*) and character set (*syb_charset*) combination you want to use.
   - If an entry does not exist, continue with step 4.
   - If an entry does exist, continue with step 5.

   Note: The value for *platform_locale* must match the value required by your operating system. If the locales definitions in your system configuration files do not match the Sybase locale definitions, your applications do not run properly.

   For example, for Open Client messages to appear in French, when Adaptive Server is using the ROMAN8 character set, check the `locales.dat` entries for your platform and look for:

   ```
   locale = fr_FR, french, roman8
   ```
4. Add the required entry or modify an existing entry.
5. Save the changes, if any, and exit the text editor.

Changing Adaptive Server and Backup Server Localization Configuration

By default, the Adaptive Server and Backup Server configurations use the English locale settings localization.

1. Start Server Config at **Start** > **Programs** > **Sybase** > **Adaptive Server Enterprise** > **Server Config**.
2. Click the icon for the server for which you want to change configuration, and click its corresponding **Configure** button.
3. Select the name of the server you want to configure, and click **Continue**.
4. Log in, if necessary.
   a) Enter the login name and password of a user with system administrator privileges, then click **Continue**.
   b) Click **Yes** if the Adaptive Server is not running.
5. Complele the localization changes for the Adaptive Server or the Backup Server.

Completing Adaptive Server Localization Changes

Each language uses about 2MB of database space per module. If necessary, use the **alter database** command to increase the size of the `master` database before adding another language.

Note: If you want to install more than one language on Adaptive Server, and the `master` database is not large enough to manage more than one language, the transaction log may become too full. You can expand the `master` database only on the master device. See the *System Administration Guide: Volume 2*.

1. Start Server Config.
2. Choose **Language**.

   Note: If you change the sort order or default character set, you must reconfigure existing databases to work with the new data requirements. See the *System Administration Guide: Volume 1*.

3. Click the appropriate **Add/Remove** option.

   You see the Install Languages or Install Character Sets dialog box, depending on your choice. The languages and character sets that appear in the Selected list are already installed and available for Adaptive Server to use.

   You can configure only those languages for which message files exist. Some languages that do not have message file cannot be installed using the Server Config utility. If your language does not appear as one of the available languages, exit Server Config and install a new language module.

   a) Select a language or character set from the Available list, and click **Add** or **Remove**.
   b) Click **OK**. The Configure Adaptive Server dialog box redisplays.

   Note: The Japanese language cannot coexist with any other installed language. If you install the Japanese language on Adaptive Server, you must make it the default language.

4. To change the default language, character set, or sort order, click the appropriate **Set Default** button.
5. For languages or character sets:

   a) Select an option from the Available list, and click **Add**.
   b) Click **OK**.

   For sort orders:

   a) Select a sort order from the Available Sort Orders list.
   b) Click **OK**.

6. In the Language Options dialog box, click **OK**.
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.

Completing Backup Server Localization Changes

When you select the Backup Server to configure, Server Config displays the Configure Backup Server dialog box.

1. From the Configure Backup Server dialog box, select the default language and character set.
2. Click **Save** to return to the Configure Sybase Servers dialog box.
3. When you have completed the necessary configuration changes, click **Exit** to quit Server Config.

Configuring Adaptive Server for Other Character Sets

Configure Adaptive Server with the character set and sort order for your language. Your system messages appear in the default language, English.

Prerequisites

To use the **charset**, the server must be running and you must have System Administrator privileges. Use the *file name* of the sort order:

```
%SYBASE%\%SYBASE_ASE%\bin\charset -Usa -Ppassword -Sserver_name
sort_order_file character_set
```

Replace *sort_order_file* with the name of the sort order file. Replace *character_set* with the Sybase name for your character set.

Task

1. Use the **charset** utility to load the default character set and sort order.
2. Use **charset** to load any additional character sets.

   If you plan to use the Adaptive Server built-in character set conversions, you must load the character set definition files for all the characters set on your client platforms. If you are using the Unilib character set conversions, you do not need to do this.
3. Use **isql** to log in to your server as “sa” and select the master database.

   ```
   1> use master 2> go
   ```
4. Use the *ID* of the sort order to configure your server for the new character set and sort order.

   ```
   1> sp_configure "default sort_order_id",
   2> sort_order_id, "character_set"
   3> go
   ```

   Replace *sort_order_id* with the ID for your sort order.

Replace *character_set* with the Sybase name for your character set.

5. Shut down the server to start the reconfiguration process.
6. Restart the server. Use Windows Service Manager from your Sybase Program Group or from a command prompt, invoke RUN_`server_name.bat` from `%SYBASE%\%SYBASE_ASE%\install`.
7. Restart a second time to bring the server up in a stable state.

See also

- *charset Utility* on page 77
- *Available Sort Orders* on page 65
- *Sybase Character Set Names* on page 75

Language-Specific Sort Orders

Available sort orders.

Language or Script	Sort Orders	File Name	ID
All languages	Binary order	`binary.srt`	50
Cyrillic	Dictionary order, case-sensitive, accent-sensitive	`cyrdict.srt`	63
	Dictionary order, case-sensitive, accent-sensitive	`cyrnocs.srt`	64
English French German These sort orders work with all Western European character sets.	Dictionary order, case-sensitive, accent-sensitive	`dictiona.srt`	51
	Dictionary order, case-insensitive, accent-sensitive	`nocase.srt`	52
	Dictionary order, case-insensitive, accent-sensitive, with preference	`nocasepr.srt`	53
	Dictionary order, case-insensitive, accent-insensitive	`noaccent.srt`	54

Language or Script	Sort Orders	File Name	ID
English French German These sort orders work only with CP 850.	Alternate dictionary order, case-sensitive	alt-dict.srt	45
	Alternate dictionary order, case-sensitive, accent-insensitive	alt-noacc.srt	39
	Alternate dictionary order, case-sensitive, with preference	alt-nocsp.srt	46
Greek This sort order works only with ISO 8859-7.	Dictionary order, case-sensitive, accent-sensitive	ell-dict.srt	65
Hungarian These sort orders work only with ISO 8859-2.	Dictionary order, case-sensitive, accent-sensitive	hun-dict.srt	69
	Dictionary order, case-insensitive, accent-sensitive	hun-noac.srt	70
	Dictionary order, case-insensitive, accent-insensitive	hun-nocs.srt	71
Russian This sort order works with all Cyrillic character sets except for CP 855.	Dictionary order, case-sensitive, accent-sensitive	rus-dict.srt	58
	Dictionary order, case-insensitive, accent-sensitive	rus-nocs.srt	59
Scandinavian These sort orders work only with CP 850.	Dictionary order, case-sensitive, accent-sensitive	scan-dict.srt	47
	Dictionary order, case-insensitive, with preference	scan-nocp.srt	48

Language or Script	Sort Orders	File Name	ID
Spanish	Dictionary order, case-sensitive, accent-sensitive	es-pdict.srt	55
	Dictionary order, case-insensitive, accent-sensitive	es-pnocs.srt	56
	Dictionary order, case-insensitive, accent-insensitive	es-pnoac.srt	57
Thai	Dictionary order	dic-tion-ary.srt	51
Turkish These sort orders work only with ISO 8859-9.	Dictionary order, case-sensitive, accent-sensitive	tur-dict.srt	72
	Dictionary order, case-insensitive, accent-insensitive	turn-oac.srt	73
	Dictionary order, case-insensitive, accent-sensitive	turn-ocs.srt	74

Sybase Character Set Names

Supported character sets and their Sybase name.

Character Sets	Sybase Name
ASCII 8	acsii_8
Big 5	big5
CP 437	cp437
CP 850	cp850
CP 852	cp852
CP 855	cp855
CP 857	cp857
CP 860	cp860

Character Sets	Sybase Name
CP 863	cp863
CP 864	cp864
CP 866	cp866
CP 869	cp869
CP 874	cp874
CP 932	cp932
CP 936	cp936
CP 950	cp950
CP 1250	cp1250
CP 1251	cp1251
CP 1252	cp1252
CP 1253	cp1253
CP 1254	cp1254
CP 1255	cp1255
CP 1256	cp1256
CP 1257	cp1257
CP 1258	cp1258
DEC Kanji	deckanji
EUC-CNS	euccns
EUC-GB	eucgb
EUC-JIS	eucjis
EUC-KSC	eucksc
GREEK8	greek8
ISO 8859-1	iso_1
ISO 8859-2	iso88592
ISO 8859-5	iso88595
ISO 8859-6	iso88596
ISO 8859-7	iso88597

Character Sets	Sybase Name
ISO 8859-8	iso88598
ISO 8859-9	iso88599
ISO 8859-15	iso885915
Koi8	koi8
Kazakhstan Cyrillic	kz1048
Macintosh Cyrillic	mac_cyr
Macintosh Central European	mac_ee
Macintosh Greek	macgrk2
Macintosh Roman	mac
Macintosh Turkish	macturk
ROMAN8	roman8
Shift-JIS	sjis
TIS 620	tis620
TURKISH8	turkish8
UTF-8	utf8

See also

- *charset Utility* on page 77
- *Available Sort Orders* on page 65
- *Configuring Adaptive Server for Other Character Sets* on page 72

charset Utility

Use the **charset** utility to load character sets and sort orders into Adaptive Server during installation.

To change the default character set and sort order of Adaptive Server, see the *System Administration Guide: Volume 1*.

Syntax

```
charset
[ -U username ]
[ -P password ]
```

```
[ -S server ]
[ -I interfaces ]
[ -v version ]
sort_order
[charset]
```

Table 5. Keywords and Options for charsets

Keywords and Options	Description
`-U`	If you are not already logged in to your operating system as "sa", you must specify `-Usa` in the command line.
`-P`	Specifies the "sa" password on the command line. If not specified, the user is prompted for the "sa" password.
`-S`	Specifies the name of the server. If not specified, **charset** uses the DSQUERY environment variable to identify the server name. If there is no DSQUERY environment variable, **charset** attempts to connect to a server named "SYBASE."
`-I`	Specifies the `interfaces` file to use. If not specified, **charset** uses the `interfaces` file in the `SYBASE` directory.
`-v`	Prints the Sybase version string, then exits. Use with no other options specified.
sort_order	When **charset** is used to load the default character set and sort order, *sort_order* is a mandatory parameter specifying the name of the sort order file to be used by Adaptive Server. When loading additional character sets, use `charset.loc` to indicate the name of the character set files.
charset	Specifies the directory of the character set to be used by Adaptive Server.

See also

- *Available Sort Orders* on page 65
- *Sybase Character Set Names* on page 75
- *Configuring Adaptive Server for Other Character Sets* on page 72

CHAPTER 13 Log Error Messages and Events

Adaptive Server supports Adaptive Server error logging and Windows event logging.

Adaptive Server Error Logging

Upon start-up, Adaptive Server begins to write information to a local error log file: %SYBASE%\%SYBASE_ASE%\install\errorlog.

This 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

If this file becomes too large, you can:

- Use **sp_errorlog** to dynamically change its path. Once the older error log is not being used by Adaptive Server, you can move it, and make space available.
- Stop the Adaptive Server and delete logged messages.

See *Diagnosing System Problems* in the *System Administrator Guide, Volume 1* for a description of the error log format.

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.

Adaptive Server error log stores:

- 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

Windows Event Logging

Adaptive Server logs error messages in the Windows event log, if event logging is enabled.

Windows event logging can:

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

Setting Up Windows Event Logging

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

1. Select **Start** > **Programs** > **Administrative Tools** > **Event Viewer**.
2. Select **Log** > **Log Settings**.

   In Event Log Settings dialog box, make sure **System Log** is selected.
3. Change the Maximum Log Size to 2048, if necessary.
4. Click the **Overwrite Events as Needed** button to toggle the feature on.
5. Click **OK**.
6. Select **Log** > **Exit**.

Enable and Disable Windows Event Logging

By default, Adaptive Server enables message logging to the Windows event log at start-up. You can disable and enable logging of Adaptive Server messages to Windows using either Server Config or**sp_configure**.

Enabling or Disabling Event Logging Using Server Config Utility

Use Server Config utility to control event logging.

1. Select **Start** > **Programs** > **Sybase** > **Adaptive Server Enterprise** > **Server Config**.
2. Click the **Adaptive Server** icon, then **Configure Adaptive Server**.
3. Select server to configure, and click **Continue**.
4. Enter the login name and password of an Adaptive Server user with system administrator privileges, then click **Continue**.
5. When prompted, click **Yes** if the Adaptive Server is not running.
6. Click **Event Logging**.
7. Click **Use Windows Event Logging** to enable or disable Adaptive Server error message logging to the Windows event log.
8. In the Event Log Computer Name field:
   a) To send messages to a remote computer log, enter its name.
   b) To send messages to a local computer log, let the value default to **LocalSystem**.
9. Click **OK**.
10. Click **Save** then click **Exit**.

Enabling or Disabling Event Logging Using sp_configure

You can enable Adaptive Server message storage in the Windows event log by using **sp_configure** to set the **event logging** configuration parameter.

Possible values are:

- 1 – enable logging of Adaptive Server messages:
  ```
  sp_configure "event logging", 1
  ```
- 0 – 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**, see the *System Administration Guide: Volume 1*.

Windows Event Log Information

Adaptive Server logs the same messages in the Windows event log as in the Adaptive Server error log, with the exception of normal start-up messages: only start-up messages are recorded in the Windows event log.

Optionally, you can record successful and unsuccessful logins to Adaptive Server in both the Adaptive Server error log and the Windows event log.

Manage Logs

Parameters, options, and system procedures for enabling and disabling event and error logging and whether they affect the Adaptive Server error log, Windows event log, or both.

Table 6. Methods for Enabling/Disabling Error and Event Logging

Method	Affects Event Log	Affects Error Log
error logging configuration parameter	Yes	No
event log computer name configuration parameter	Yes	No
Server Config Event Logging option	Yes	No
Server Config Error Log Path option	No	Yes
sp_altermessage system procedure	Yes	Yes
sp_addmessage system procedure	Yes	Yes

Method	Affects Event Log	Affects Error Log
log audit logon success configuration parameter	Yes	Yes
log audit logon failure configuration parameter	Yes	Yes
xp_logevent system extended stored procedure	Yes	No

Set Error Log Paths

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

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

- Adaptive Server: %SYBASE%\%SYBASE_ASE%*installation directory*
- Backup Server: %SYBASE%\%SYBASE_ASE%*installation directory*

At start-up, you can reset the name and location of the Adaptive Server error log file from the command line by using the `-e` start-up parameter.

Note: Multiple Adaptive Servers cannot share the same error log. If you install multiple Adaptive Servers, 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 Adaptive Server error log path.

1. Select **Start > Programs > Sybase > Adaptive Server Enterprise > Server Config**.
2. Click the **Adaptive Server** icon from the Products box.
3. Click **Configure Adaptive Server**.
4. Select the server to configure, then click **Continue**.
5. Enter the login name and password of an Adaptive Server user with system administrator privileges, then click **Continue**.
6. When prompted, click **Yes** if Adaptive Server is not running.
7. Click **Error Log Path**, then enter the full path name to an error log file that is not on a network drive. Click **OK**.
8. Click **Save**, then click **Exit**.

Setting the Backup Server Error Log Path

Use the Server Config utility to change the Backup Server error log path.

1. Select **Start > Programs > Sybase > Adaptive Server Enterprise > Server Config**.

2. Click the **Backup Server** icon from the Products box in the Configure Sybase Servers dialog box.
3. Click **Configure Backup Server**.
4. Select the server to configure, then 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.
6. Click **Save**, then click **Exit**.

Manage Messages

When event logging is enabled, you can manage its functions.

You can:

- Use **sp_addmessage** to add a user message, or **sp_altermessage** to control whether a specific message is logged in both the Adaptive Server error log and in the Windows event log.
  For the complete syntax for the **sp_addmessage** and **sp_altermessage** system procedures, see the *Reference Manual: Procedures*.
- 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 in to Adaptive Server.
- Use the **xp_logevent** extended stored procedure to set up logging of user-defined events in the Windows event log in Adaptive Server.

Log 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 event log.

Adaptive Server lets you make this determination for:

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

See **sp_addmessage** and **sp_altermessage** in the *Reference Manual: Procedures*.

New Messages

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

Existing Messages

Include the **with_log** option in **sp_altermessage** to change an existing user-defined message.

This parameter alters the reporting status of that message:

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

Log 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 Windows 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 **sp_configure**, see the *System Administration Guide: Volume 1*.

Log User-Defined Events

You can arrange to have user-defined events logged to the Windows 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, including:

- 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

See **xp_logevent** in the *Reference Manual: Procedures*.

Using a Remote Log

By default, if event logging is enabled, Adaptive Server logs messages to the Windows event log on the local computer system. You can change the destination computer to which to log messages.

1. On a local computer, either:
   - Use **sp_configure**, as in the following command line, or:
     ```
     sp_configure "event log computer name", 0, user1
     ```

or,

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

2. Start the server from a Domain Administrators account.

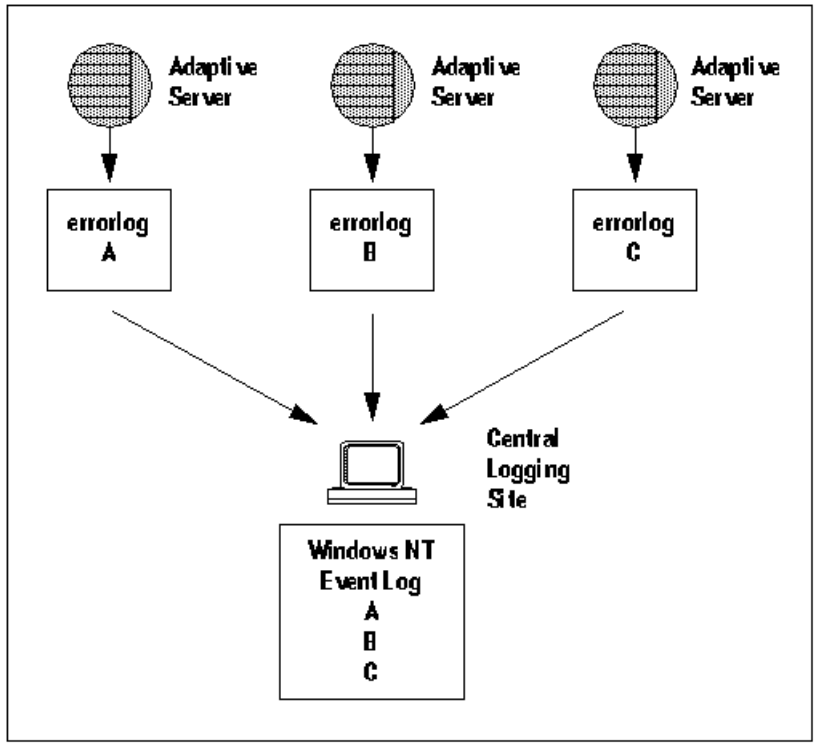
a) Choose **Start > Settings > Control Panel > Services**.
b) Select the remote server to use.
c) Click **Startup**.
d) In the **Log On As** field, click **This Account In**.
e) Click the drop-down list to display the Add Users dialog box.
f) Double-click an account name in the Domain Administrators group, then 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.

Central Logging Site

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

Figure 3: Diagram of a Central Logging Site



Use a central logging site for 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 can view error messages in either the local Adaptive Server error log file or the central event logging site.

Log Messages from Multiple Adaptive Servers

Configure central logging computer 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

Set Up a Local Central Logging Site

An event-logging computer uses a Registry key to define each message-sending Adaptive Server, and cannot log messages from servers for which it has no key.

Creating a Registry key

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

1. Log in to Windows using an account with Windows administrator privileges.
2. Copy the `sybevent.dll` file from an Adaptive Server machine if it does not already 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 Windows 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 15.0.3.
3. Start the Windows **regedt32** utility.
4. Select the Registry window named HKEY_LOCAL_MACHINE.
5. Open the levels until you reach the Registry key named:

   HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\EventLog \Application
6. Select **Edit** > **Add Key**.
7. Complete the **Add Key** dialog box:
   - Key Name – enter the name of the Adaptive Server computer that is to store the messages at the central logging site.
   - Class – leave blank.
8. Click **OK**.

Next

Define the key that you just created.

Defining a Registry Key

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

Prerequisites

Create a Registry key in the **regedt32** utility.

Task

1. Start the Windows **regedt32** utility.
2. In the **regedt32** utility, open the Registry key that you just created.
3. Select **Edit** > **Add Value**.
4. Type an event-logging value name for the new Registry key. Enter the value name exactly as it is shown in the table; value names are case-sensitive.

Table 7. 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`	`%SYBASE%\%SYBASE_ASE%\dll directory`	Replace `%SYBASE%\%SYBASE_ASE%\dll directory` with the path to the `sybevent.dll` file.
EventMessageFile	`REG_SZ`	`%SYBASE%\%SYBASE_ASE%\dll directory`	Replace `%SYBASE%\%SYBASE_ASE%\dll directory` 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.

5. Select the datatype for each value.
6. Verify that you have entered the new key value and datatype correctly, and click **OK**.
7. Enter the appropriate string, and click OK.
8. Repeat steps 5-9 for the remaining three values in each Registry key.
9. Select **Registry > Exit**.

View Messages

Use the Windows Event Viewer and a text editor to look at and log error messages.

Viewing Messages in the Windows Event Log

Use the Windows Event Viewer in the Administrative Tools group to view messages.

1. Select **Start > Administrative Tools > Event Viewer**.
2. Double-click a message to see details.

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

Viewing Messages 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.

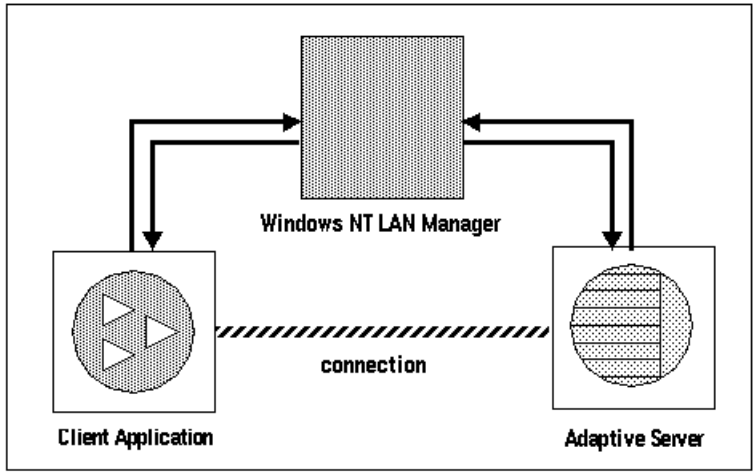
1. Select **Start > Programs > Sybase > Server Config**.
2. Click the **Adaptive Server** icon, then click **Configure Adaptive Server**.
3. Select server for which to examine the error log, then click **Continue**.
4. Enter the login name and password of an Adaptive Server user with system administrator privileges, then click **Continue**.
5. When prompted, click **Yes** if the Adaptive Server is not running.
6. Click **Error Log Path**.

See the *System Administration Guide: Volume 1*.

CHAPTER 14 Security Services with Windows LAN Manager

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

Figure 4: Establishing Secure Connections Between LAN Manager and Adaptive Server



You can use secure connection between LAN Manager and a server 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 each time they log in to Adaptive Server.

The secure connection also can support one or more of these 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 validates the login with LAN Manager, Adaptive Server establishes a secure connection between itself and the client.

When a client requests authentication services:

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 with the client.

Administering Security Services Using LAN Manager

Administer the Adaptive Server unified login capability with LAN Manager.

Prerequisites

Adaptive Server must be installed before completing these step.

Task

Table 8. 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.	*Modify Configuration Files Required for a Unified Login* on page 93
2. Make sure the security administrator for LAN Manager has created logins for each user and for the Adaptive Server and Backup Server.		*Identify Users and Servers to LAN Manager* on page 96
3. Use **sp_configure** to enable security for the installation.		*Configure Adaptive Server for LAN Manager Security* on page 96
4. Restart Adaptive Server.	Activates the **use security services** parameter.	*Chapter 7, Start and Stop Servers* on page 19
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**.	*Add Logins to Support Unified Login* on page 101

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 user name or password.	*Define the Connection to a Server for Security Services* on page 102 *Open Client/Server Configuration Guide for Desktop Platforms* *Security Features* in the *Open Client Client-Library Reference Manual*

Modify Configuration Files Required for a Unified Login

Configuration files are created during installation at a default location in the Sybase directory structure.

Table 9. 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.	`%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.	`%SYBASE%\ini`
`sql.ini`	The `sql.ini` file contains connection and security information for each server that it lists.	`%SYBASE%\ini`

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

See also

- *Configure Adaptive Server for LAN Manager Security* on page 96
- *Define the Connection to a Server for Security Services* on page 102
- *Add Logins to Support Unified Login* on page 101
- *Identify Users and Servers to LAN Manager* on page 96

Set Up Drivers for Network-Based 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.

The `libtcl.cfg` file stores information about:

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

Entries for Network Drivers

Network driver entries includes driver, protocol, and description syntax.

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 an optional description of the entry.

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

Entries for Directory Services

Use directory entries only if you want to use a directory service instead of the `sql.ini` file.

Warning! Client applications bundled with Adaptive Server require a `sql.ini` file for effective processing. Eliminating this file with a directory service may limit Adaptive Server functionality.

Entries for Security Drivers

The security driver entries include provider and driver syntax.

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 Windows LAN Manager on Windows 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.

- *driver* is the name of the security driver. The Windows LAN Manager driver is named "LIBSMSSP." The default location of all drivers is `%SYBASE%\%SYBASE_OCS%\dll`.

Editing the libtcl.cfg File

Use the **ocscfg** utility to edit the `libtcl.cfg` file.

For information about 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: 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.

This 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, which provides a graphical user interface for specifying server attributes such as the server version, name, and security mechanism.

See the *Open Client/Server Configuration Guide for Desktop Platforms*.

Identify 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 need not enter the Adaptive Server name as a principal to LAN Manager. However, the Windows user account that you use to start Adaptive Server must be defined as a valid principal to LAN Manager. For example, to use an Windows 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 Windows service. See the *Installation Guide*.

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

See also

- *Configure Adaptive Server for LAN Manager Security* on page 96
- *Define the Connection to a Server for Security Services* on page 102
- *Add Logins to Support Unified Login* on page 101
- *Modify Configuration Files Required for a Unified Login* on page 93

Configure 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

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 the *Installation Guide*.

See also

- *Define the Connection to a Server for Security Services* on page 102
- *Add Logins to Support Unified Login* on page 101

- *Identify Users and Servers to LAN Manager* on page 96
- *Modify Configuration Files Required for a Unified Login* on page 93

Enabling and Disabling External Security Services

Reset the LAN Manager security service using **sp_configureuse security services**.

- 1 – enable services with LAN Manager.
- 0 – (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
```

Manage Unified Login

Use the unified login configuration parameters to require unified login, and to establish a default secure login. These parameters take effect as soon as you change them.

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 – require all users who request a connection to Adaptive Server to be authenticated by LAN Manager.
- 0 –(default) allow 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 in to Adaptive Server, the server checks whether the name is listed as a user in `master..syslogins`. If it is, Adaptive Server accepts that user name.

1. 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”.

2. 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”.
3. 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: gen_auth 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 example, a user logs in to 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 in to 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.

Map 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 invalid 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 10. Conversion of Invalid Characters in Login Names

Invalid Character	Converts to
Ampersand & Apostrophe ' Backslash \ Colon : Comma , Equals sign = Left single quotation mark ‘ Percent sign% Right angle bracket > Right single quotation mark ’ Tilde ~	Underscore _
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 *Reference Manual: Blocks*.

Data Integrity Check

Use configuration parameters with LAN Manager to check one or more types of data integrity for all messages.

- **msg integrity reqd**– set to 1 to force a check for general tampering in all messages.
  If the parameter is 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 to 1 to force a check for sequence changes in all messages.
  If the parameter is 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 to 1 to force a check for replay or interception in all messages.
  If the parameter is 0 (the default), replay detection is not required. However, the client can establish this check if the security mechanism supports it.

Ensure 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 there is sufficient memory when using unified login and security services through LAN Manager, allocate approximately 6K of additional memory per connection.

For example, if the maximum number of unified logins that occur simultaneously 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 information about estimating and specifying memory requirements for Adaptive Server, see the *System Administration Guide: Volume 2*.

Add Logins to Support Unified Login

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.

When a user logs in to Adaptive Server with an authenticated credential, Adaptive Server:

1. Checks that the user is a valid user in `master..syslogins`.
   - If the user name 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.

Note: You must add the default login in `master..syslogins` and use **sp_configure** to define the default.

See also

- *Configure Adaptive Server for LAN Manager Security* on page 96
- *Define the Connection to a Server for Security Services* on page 102
- *Identify Users and Servers to LAN Manager* on page 96
- *Modify Configuration Files Required for a Unified Login* on page 93

Adding Logins

To add logins to the server and, optionally, to add users with appropriate roles and authorization to one or more databases you must meet the required role to follow the command or procedure.

Prerequisites

Ensure that you have the required role and authorization to perform each step assigned to you.

Task

See the referenced documents for details.

1. Add a login for the user.
   - Role: System security officer
   - Procedure: **sp_addlogin**
   - See: *Security Administration Guide*

2. Add the user to one or more databases.
   - Role: System security officer, system administrator, or database owner
   - Procedure: Run **sp_adduser** from within the database.
   - See: *Security Administration Guide*
3. Add the user to a group in a database.
   - Role: System security officer, system administrator, or database owner
   - Procedure: Run **sp_changegroup** from within the database.
   - See: *Security Administration Guide*, and *Reference Manual: Commands*.
4. Grant system roles to the user.
   - Role: System security officer, or system administrator
   - Procedure: **grant role**
   - See: *Security Administration Guide*, and *Reference Manual: Commands*.
5. Create user-defined roles and grant the roles to users.
   - Role: System security officer
   - Procedure: **create role**, and **grant role**
   - See: *Security Administration Guide*, and *Reference Manual: Commands*.
6. Grant access to database objects.
   - Role: Database object owner
   - Procedure:
     grant [**select** | **insert** | **delete** | **update**| **references** | **execute**]
   - See: *Security Administration Guide*

Define the Connection to a Server for Security Services

Define the connection to a server for security services by specifying the principal name for Adaptive Server, network-based user authentication, and the name assigned to LAN Manager through the **isql** and **bcp** utilities.

Use the following options to define an Adaptive Server for network-based security services such as Windows 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 the *Utility Guide*.

See also

- *Configure Adaptive Server for LAN Manager Security* on page 96
- *Add Logins to Support Unified Login* on page 101
- *Identify Users and Servers to LAN Manager* on page 96

- *Modify Configuration Files Required for a Unified Login* on page 93

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 in to Windows LAN Manager before running the utility. If a user specifies the **-U** option, he or she must also 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 in to LAN Manager and then log in to Adaptive Server, you do not need to specify the `-U` (user) option on the utility because Adaptive Server gets the user name from LAN Manager.

Determining the Status of Security Services

Determine whether security services are enabled for the current session, by using **show_sec_services**

In this 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

Unified login and security services use configuration parameters through LAN Manager that provide security checks.

Use:

- **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: Volume 1*.

Data Integrity Check

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.

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

Summary Information	
Required role	System Security Officer

Message Sequence Check

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.

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

Detect Interception or Replay

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.

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

Specify a Login

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

Summary Information	
Name in pre-11.0 version	N/A

Summary Information	
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

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
```

Control User Authentication

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.

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

Manage Login Security on an Windows Computer

You can use Adaptive Server security features alone or with Windows security features.

For more information about system security, see the *Security Administration Guide*.

Adaptive Server Security

Storing login information, requiring client applications to specify the login name and password of a database user, and checking the user name and password are the ways Adaptive Server enforces security.

As a standalone product, Adaptive Server ensures security by:

- Storing login information for all database users in the `master.dbo.syslogins` table. Stored passwords 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 user name and password against the information in `syslogins`, and accepting or rejecting the login accordingly.

Combined Adaptive Server and Windows Login Security

Adaptive Server increases security by integrating the default Adaptive Server login process with Windows security features.

The resulting integrated security modes add the following conveniences for users:

- Authorized users need not maintain separate login passwords for Adaptive Server and Windows.
- System administrators can take advantage of Windows security features such as encrypted passwords, password aging, domain-wide user accounts, and Windows-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 **sp_grantlogin** to assign permissions to Windows users and groups. **sp_grantlogin** lets system administrators:

- Assign one or more Adaptive Server roles to Windows users and groups
- Designate 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.

Note: Adaptive Server does not permit trusted connections for Windows users named "sa." The user name "sa" is reserved for the default Adaptive Server system administrator account.

Login Security Modes

Adaptive Server provides Standard, Integrated, and Mixed modes for configuring login security.

Standard Mode

In Standard mode, Adaptive Server manages its own login validation process for all connections.

This is done by:

- Ignoring the Windows network user name and checking the supplied Adaptive Server user name 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 *Security Administration Guide*.

Integrated Mode

In Integrated mode, Adaptive Server uses Windows-based authentication mechanisms for all connections.

This is done 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 Windows network user name against the information in the `syslogins` table.

  If no matching login name exists, and the login process includes a default user name, Adaptive Server substitutes the default login name, for example, "guest", to complete the connection.
- Providing authorized users, when they log in, with permissions and roles.
- Following the Windows Domain structure for the use of computers. Windows must authenticate each user, either through trust relationships or through explicitly assigned permissions on each server.

Note: If you bypass Windows 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

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, depending on the information supplied, handles the login.

Adaptive Server processes the login:

- When the login name matches the mapped network user name, 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 user name 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.

Manage the Login Security Features

Use the trusted connections and Windows Registry parameters to manage login security in Integrated or Mixed mode.

Permit 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 Windows 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 Windows 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 Windows 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 Windows users or their associated Windows groups must have permissions that were assigned with **sp_grantlogin**.

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

Windows 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 in Integrated or Mixed mode.

Management parameters include:

- Default login
- Default domain
- SetHostName
- Character mappings

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 user name 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 user name in `syslogins`.

See also

- *Character Mappings* on page 111
- *Default Domain* on page 110
- *Enabling Integrated or Mixed Login Security Mode* on page 117

Default Domain

Adaptive Server uses the default domain parameter to specify the Windows or LAN Manager domain name for matching network user names to Adaptive Server login names.

Because two different domains can define the same network user name 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 user names 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 user name before looking for the user name in the `syslogins` table.

For example, the domain MARKETING is the Adaptive Server default definition, and two different users employ the network user name "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.

See also

- *Character Mappings* on page 111
- *Default Login* on page 110
- *Enabling Integrated or Mixed Login Security Mode* on page 117

SetHostName

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

- 1 (enabled) – include the network user name in the results of the **sp_who** system procedure.
- 0 (disabled) – (default) omit the network user name 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 information about **regedt32**, see your Windows operating system documentation.

Character Mappings

Certain characters that are valid for Windows user names are invalid in Adaptive Server login user names.

Such characters include:

- 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 Windows user name “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 user name 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.

Table 11. Default Mapping Values

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

See also

- *Default Domain* on page 110
- *Default Login* on page 110
- *Enabling Integrated or Mixed Login Security Mode* on page 117

Modify the Parameter Values

To modify the values for the default login, default domain, and SetHostName parameters, use the Server Config or **regedt32** utility.

Note: You can change the SetHostName value only by using **reged32**.

- Use the Server Config utility to modify the value only for Adaptive Server.
- Use the **regedt32** utility to change the value directly for use throughout your Windows operating system.

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

Administer Login Security Using System Procedures

You can administer integrated security from Windows.

You can:

- Assign trusted connection permissions – **sp_grantlogin**

- Display Adaptive Server integrated login configuration– **sp_loginconfig**
- Display permissions and user names – **sp_logininfo**
- Revoke permissions – **sp_revokelogin**

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

Assigning Trusted Connection Permissions

Assign permissions to Windows 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.

1. To assign the System Administrator and System Security Officer roles to all members of the Windows group named Administrators, enter:

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

2. Then, to assign “select” permissions on the `sales` table to the Windows user, “hasani”, enter:

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

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

Display the Current Registry Values

To display the current settings for the Registry values, use **sp_loginconfig**.

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 #                  -
```

Display Permissions and User Names

To display the current permissions and mapped user names for both Windows users and groups, use **sp_logininfo**.

A sample listing of permissions and user names:

```
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 Windows administrators group: **sa_role**, **sso_role**, and **oper_role**.
  - The group names are prefaced by "BUILTIN\" to indicate that the entry refers to a built-in Windows group (a default group on all servers), rather than a group that is created by the user.
  - 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 Windows group, but you do need to add a login for each user in that group.
- The first Windows 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 Windows user, also named "chantal", logs in from the EAST domain. Her mapped user name 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 users, groups, and permissions use the **sp_grantlogin** and **sp_revokelogin** procedures.

Revoke Permissions Granted with sp_grantlogin

Use **sp_revokelogin** or **revoke** to revoke permissions that were granted with **sp_grantlogin**.

Use:

- 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.

This command line revokes all permissions from the Windows group named Administrators:

```
sp_revokelogin Administrators
```

Configuring Login Security

There are a variety of ways to configure login security.

Sybase recommends that you set up login security in this order:

1. Create Windows users and groups.
2. Configure mapping and default domain values.
3. Set login security mode.
4. Add network login names to **syslogins**.
5. Assign roles.

Creating Windows Users and Groups

User account and user groups that access Adaptive Server over trusted connections are created with User Manager.

Start User Manager from **Start** > **Programs** > **Administrative Tools**.

When creating groups and users:

- Make sure that Windows users and groups exist before you assign permissions to them in Adaptive Server.
- Create the accounts with a user name other than “sa”.

  Note: Some functions are divided between**sa_role** and **sso_role**. You may want to assign both roles to Adaptive Server system administrators to provide the same permission level. For more information, see the *System Administration Guide: Volume 1*.
- 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 Windows 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 Windows users. After you become more experienced with administering integrated security, you can expand the permission levels to include Windows groups.

Configuring Mapping and Default Domain Values

Change login security options to set the mapping and default domain options.

Configure these values before adding accounts to Adaptive Server, as these values affect the format of entries in `syslogins`.

For example, a user named "joseph" in the WEST domain is to log in to 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".

Setting Login Security Mode

Change login security options to set the security mode to either Integrated or Mixed.

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 in to Adaptive Server using standard Adaptive Server user names and passwords, such as the user name "sa".

Adding Network Login Names to syslogins

To add a login name for each Windows user accessing Adaptive Server over a trusted connection, use **sp_addlogin**. Include any nondefault 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 **sp_logininfo** to determine the format of entries in `syslogins`.
3. Use the entries listed in the `mapped login name` column as templates for the login names you create with **sp_addlogin**.

Assigning Roles

To assign roles or "default" permissions to Windows users or groups, use **sp_grantlogin**. Keep in mind that assigning permissions to Windows 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.

Change Login Security Options

When you install a new Adaptive Server, the installation program sets it to operate in Standard mode.

Use Server Config to change:

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

Enabling Standard Login Security Mode

Specify the login security mode.

1. Log in to Windows using an account with Windows administrator privileges.
2. Start the Server Config utility.
3. Complete the initial steps to configure Adaptive Server.
4. Click **Login Security** in the Configure Adaptive Server Enterprise dialog box.
5. Click **Standard**, then click **OK**.
6. Click **Save**, then **Exit**.

Enabling Integrated or Mixed Login Security Mode

Specify the login security mode.

1. Log in to Windows using an account with Windows administrator privileges
2. Start the Server Config utility.
3. Complete the initial steps to configure Adaptive Server.
4. Click Login Security in the Configure Adaptive Server Enterprise dialog box.
5. Click Integrated, then click Continue.
6. Set the login security mode:
   - Integrated mode – click **Automatic Login for Trusted Connections (Named Pipes) Only option**.
   - Mixed Media mode – click **Trusted First and Adaptive Server Login for Excluded (i.e., NetWare, TCPIP)**.
7. Enter the name of the default user account to use for trusted connections. Adaptive Server uses this value when it cannot locate the user name in `syslogins`.
8. Enter either the default domain name or the workstation's network name.
9. Click **Map Characters** to configure Adaptive Server mappings under an Integrated security mode.
10. Select any invalid character to be mapped to each valid Adaptive Server character.
11. Click **OK** several times to exit from the dialog boxes. Then click **Save**, and **Exit** to quit Server Config.

See also

- *Character Mappings* on page 111
- *Default Domain* on page 110
- *Default Login* on page 110

CHAPTER 15 E-mail Messages and Adaptive Server

Adaptive Server can send and receive e-mail messages through Sybmail, the Sybase messaging facility, and can also take advantage of Windows Mail.

Sybmail Messages

Adaptive Server for Windows can send, receive, and process e-mail messages.

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.

Send Messages

Messages from Adaptive Server (outgoing messages) can be either text or formatted query results.

The Adaptive Server 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 reordered 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.

Receive Messages

The Adaptive Server 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 Windows Mail for Sybmail

Sybmail uses Windows Mail facility, so you must prepare the Windows Mail system before you can use Sybmail.

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

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

Connecting to a Post Office

A Windows post office holds messages until recipients retrieve them.

The computer that is running Adaptive Server must have access to an Windows 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, be prepared to supply its path.

Creating a Mailbox for Adaptive Server

After connecting to or creating a post office, create a mailbox in it for Adaptive Server.

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

Supply a mailbox name and password for the mailbox.

- The password is needed 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 create.

Creating a Mail Profile for Adaptive Server

After you have added a mailbox for Adaptive Server, 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 the Adaptive Server mailbox password.
- The mailbox name must be the one you created for Adaptive Server.

In the Mail Login Properties window, make sure **When logging on, automatically enter password** is selected.

Create an Adaptive Server Login for Sybmail

After setting up an Adaptive Server profile in Windows Mail, create a login for Sybmail on Adaptive Server.

When creating this user account, make sure:

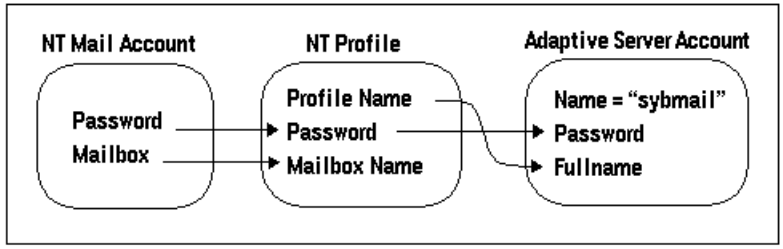
- The *loginame* parameter is "sybmail".
- The *fullname* parameter has the same value as the Profile Name for the Adaptive Server mail profile.
  Adaptive Server uses this value as its MailUserName.
- The *password* parameter has the same value as the password for the mailbox that is associated with the server's mail profile.
  This value becomes the Adaptive Server MailPassword.

These values are the defaults for starting an Adaptive Server mail session using **xp_startmail**.

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

- **sp_addlogin** from **isql**:
  ```
  sp_addlogin "sybmail", "wrtyzz2c", @fullname="sqlserver"
  ```
  or,
- The Add Login facility in Sybase Central or Adaptive Server Manager.

Figure 5: User-Defined Values Relationships in Sybmail



Configuring Sybmail and Extended Stored Procedures

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

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

1. Start the Server Config tool.
2. Complete the initial steps to configure Adaptive Server.
3. Click **Configure Default XP Server**.
4. Click **This Account**, then enter a valid Windows user account and password for the server. Make sure that the account has the right to log in as a service.

   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 Windows User Manager:

   a) Select **Start > Programs > Administrative Tools > User Manager**.
   b) Select the user name to act as the service.
   c) Select **Policies > User Rights**.
   d) Select **Show Advanced User Right**.
   e) Select **Log on as a service**, and click **OK**.
   f) Exit User Manager.
5. Click **OK**, then **Save**, then **Exit**.

Manage 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.

Start a Mail Session

When Adaptive Server starts a session, the mail user is represented by the MailUserName and the MailPassword that 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 user name 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.

Start Sybmail Without Parameters

You can start Sybmail with **xp_startmail** and no parameters (default configuration).

You can do this 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.

Stop a Mail 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 *Reference Manual: Procedures*.

Note: 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

Procedures that process e-mail for Adaptive Server.

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.

Procedure	Description
xp_stopmail	Stops an Adaptive Server mail session.
sp_processmail	Reads, executes, responds to, and deletes messages submitted to Adaptive Server by e-mail.

Outgoing 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 **xp_sendmail**.

- To send query results, input the query, or a stored procedure containing the query, to **xp_sendmail**. The query results are sent to message recipients.
- When the message consists of query results, you can send the results 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 query results 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 *Reference Manual: Procedure*.

Text Messages

This example shows how you can use a trigger to send an e-mail to "purchasing" when an update causes the number of items available (`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

The purchasing department can send the Adaptive Server mailbox a query to determine which parts should be reordered.

Adaptive Server then reads the query into a variable, named *received_mess*, 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 to a mail group.

This 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"
```

Incoming 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 Users Guide*.

Sybmail includes these ESPs to process incoming messages:

- **xp_findnextmsg**
- **xp_readmail**
- **xp_deletemail**

For complete syntax and parameters, see the *Reference Manual: Procedures*.

Find 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.

Pass the message identifier that is returned by **xp_findnextmsg** to subsequent procedures that read and delete messages.

Read 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).

Delete a Message

After reading Adaptive Server mail with **xp_readmail**, you can remove the message from the 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 manually process Adaptive Server incoming e-mail queries.

1. Call the ESPs **xp_findnextmsg**, **xp_readmail**, and **xp_deletemail** individually for each message.
2. Use **xp_sendmail** to execute the query in each message and send the e-mail results back to the requestor.

However, using **sp_processmail** invokes these ESPs automatically.

sp_processmail reads and responds to unread messages in the Adaptive Server inbox. You can determine which messages to process by passing a value for the *originator* parameter, the *subject* parameter or both.

Table 12. 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*	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 *Reference Manual: Procedures*.

This 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.

Sybmail Security

To prevent unauthorized users from accessing privileged Adaptive Server data through e-mail use the **xp_sendmail** or **sp_processmail** procedures to set the execution privileges on the ESPs that process mail and to set the security context for executing queries.

Set 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.

To prevent unauthorized users from accessing Sybmail to execute queries that they would normally not be able to execute, limit execution permission of these procedures to users with the **sa_role** or to a very small group of users.

Set the Execution Context

When you use **xp_sendmail** to execute a query that has been submitted via an e-mail message, 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 these variables:

- *dbuser* – to reset the login name, which must represent a valid Adaptive Server account on the target Adaptive Server.
- *dbname* – to reset the database name.

Name Both the User and the Database

Specify *dbuser* and *dbname* to control how Adaptive Server executes a query.

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.

Name the User But Not the Database

Specify only *dbuser* to execute the command, **xp_sendmail**, or **sp_processmail**, in the `master` database.

When the login specified by *dbuser* is an invalid user in the `master` database, Adaptive Server executes the query in the user context of "guest".

Name the Database But Not the User

Specify only *dbname* to set the default *dbuser* as "sybmail" 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.

Name 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 16 Manage Adaptive Server Databases

The administration of Adaptive Server databases includes both routine tasks and performance and tuning considerations.

Manage 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

Device requirement constraints on the size and number of Adaptive Server devices.

For Adaptive Server devices:

- The maximum device size is 4TB.
- Each database can have up to 2G - 1devices.
- The maximum database size is 8 – 64 TB (dependent upon page size.)

Although some operating systems can designate an entire hard disk to use as a database device, Windows 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

Use the **disk init** command to specify the drive, path, and file name of a new 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 Windows service.

1. If the `d:\data` directory does not exist, create it from the Windows command prompt:

   ```
   d:\> mkdir data
   ```

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:

```
1> disk init
2> name = "user_device1",
3>physname = "d:\data\user1.dat",
4>size = 4M
5> go
```

This example creates a 4MB device 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 using "vdevno = (number)".

For more information about **sp_helpdevice** and the **disk init** command, see the *System Administration Guide: Volume 2* and the *Reference Manual: Commands*.

Note: Sybase recommends that you do not use raw partitions for database devices.

Back Up and Restore 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, use a tape drive or a hard disk, 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 the *Installation Guide*.

Note: Always use the Adaptive Server **dump database** and **load database** commands, rather than the Windows 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: Volume 2*.

Backing Up Data with a Tape Drive

Sybase software can back up and restore databases to tape drives that are compatible with Windows.

Supported tape drives that are compatible with Windows, include:

- 1/4-inch cartridge
- 4-mm and 8-mm digital audio tape (DAT) formats

1. Install the tape drive according to the manufacturer's instructions.

This task includes installing an Windows-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 Windows operating system documentation.

2. Start **isql**, and connect to Adaptive Server:

```
d:\sybase\bin> isql -Usa -Ppassword -Sserver_name
```

3. Use the Windows tape device name with **isql** statements to name the tape drive.

Windows Tape Drive Names

Windows tape devices use the format "TAPE*n*", where *n* is the tape drive number, in its physical device names.

Windows 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 Windows setup program uses these device names to create logical device names to refer to the Windows 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.

To create a new, logical device name, use the **sp_addumpdevice** system procedure.

Set the Maximum Capacity for a Tape Drive

To run properly, the **dump** command needs to know the maximum capacity of the destination tape drive.

The **dump** command 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 Windows, 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.

Backing Up Data Using a Hard Disk

Sybase software can back up data to any existing directory on a mounted Windows volume.

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.

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.

By default, all Windows 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 Windows default account. The user should have the permission to access remote drives.

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 User Databases

Use the **dump** and **load** commands for backup and recovery of Adaptive Server database on Windows.

For more information, see the *System Administration Guide: Volume 2*.

Back Up and Restore to a Database and Device

Examples demonstrating how to use a tape drive and a `.dat` file as the backup and recovery resources.

Using a tape drive

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
```

Back Up and Restore on a Remote Backup Server

An example demonstrating how to back up to and restore from the first tape drive on a remote Windows 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
```

Backup File Names

Examples about naming a backup file.

To back up a transaction log 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.

Additional Dump Devices

Examples about how to specify 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

Example of tape handling options to initialize two devices to overwrite the existing content with the new transaction log backups.

```
1> dump transaction personnel to "\\.\TAPE0"
2> stripe on "\\.\TAPE1" with init
3> go
```

Get Information About Files

Examples of getting information about the 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
```

Backing Up and Restoring System Databases

You can back up system databases the same way you back up user databases. It is not necessary to back up the `tempdb` database, as it is re-created every time the server restarts.

For more information, see the *System Administration Guide: Volume 2* and the *Transact-SQL Users Guide*

Optimize Adaptive Server Performance and Tuning

You can make changes to your Windows system to improve Adaptive Server performance. The Windows utilities let you monitor the Adaptive Server use of operating system resources —disk, memory, and I/O.

For more information, see *Performance and Tuning Series*.

Using Dedicated Adaptive Server Operation

Installing Adaptive Server on a dedicated computer improves performance, because the software does not have to share system resources with file and print server applications. However, Adaptive Server is not a foreground application, because it runs as a Windows service. Increasing the priority of Adaptive Server increases the CPU time available for the server.

1. Start the Server Config tool either from the Sybase menu or from the Sybase Central Utilities pane.

2. Select **Configure Adaptive Server**.
3. Select the server to configure, then click **Continue**.
4. If the server needs to be started, click **Yes**, and enter an "sa" login and password when prompted.
5. Select **Command Line Parameters**.
6. Enter `-P` in the parameter entry field.
7. Click **OK**.

When the server restarts, it picks up the new command line parameter.

Disk Drives and Adaptive Server Performance

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 may be unable 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.

Monitor Disk Usage

Sybase recommends, in heavily used databases, that you distribute data across multiple disks. To do this effectively, you must 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 *Reference Manual: Procedures*; also see the *System Administration Guide: Volume 2*.
- To check for disk space usage rates and I/O contention, run **sp_sysmon**.
  For more information, see **sp_sysmon** in the *Reference Manual: Procedures*; see also the *Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon*.

Monitoring Adaptive Server Statistics

You can use the Windows Performance Monitor to monitor Adaptive Server statistics. For general information about the Windows Performance Monitor, see your Windows documentation.

Prerequisites

To enable performance monitoring, make sure that the **SQL Perfmon Integration** configuration parameter is set to 1. If necessary, use **sp_configure** to reset this parameter. You must restart Adaptive Server for the setting to take effect.

Task

Note: sybperf is not supported only on 64-bit computers.

To support performance monitor integration, Adaptive Server must be registered as a Windows Service. This registration occurs automatically when you:

- Use the Services option through the Control Panel
- Have configured Windows to start Adaptive Server as an automatic service

1. Start the Windows Performance Monitor (`perfmon.exe`) from its program group.
2. Select **Edit** > **Add to Chart**.
3. If you are monitoring a local computer, go to step 4. If you are monitoring a remote computer, select it, and click **OK**.
4. Select the Adaptive Server Counter group that contains the counter to monitor.
5. Select the counter you want to monitor.

   For an explanation of a particular counter, select the counter and click **Explain**.
6. If selecting a counter displays numbers in the Instance box, select the instance want to monitor.
7. Click **Add** to activate the counter on the Performance Monitor display.

CHAPTER 17 Database Management System Auditing

Auditing is optional functionality for the Adaptive Server that tracks security-related system activity in an audit trail, which can be used to detect system penetration and system abuse.

By examining the audit trail, the system security officer can inspect patterns of access to objects in databases and monitor the activity of specific users. Audit records can be traced to specific users, enabling the audit system to act as a deterrent to users who are attempting to misuse the system.

A system security officer is the only user who can start and stop auditing, set up auditing options, and process audit data.

See also

- *sybsecurity Device and Database* on page 7

Audit System Devices and Databases

The audit system includes several components.

- The sybsecurity device and the `sybsecurity` database – stores audit information.
  The `sybsecurity` database is created as part of the auditing configuration process. It contains all the system tables in the `model` database as well as a system table for tracking server-wide auditing options and system tables for the audit trail.
- The audit trail – comprises several audit devices and tables that you configure.
  Adaptive Server stores the audit trail in as many as eight system tables, named `sysaudits_01` through `sysaudits_08`.
  For example, if you have two audit tables, they are named `sysaudits_01` and `sysaudits_02`. At any given time, only one is current. Adaptive Server writes all audit data to the current audit table. A system security officer can use **sp_configure** to set or change the current audit table.
  When you configure Adaptive Server for auditing, determine the number of audit tables for your installation. Plan to use at least two or three system tables for the audit trail and to put each system table on its own device, separate from the master device. This allows you to use a threshold procedure that archives the current audit table automatically, before it fills up and switches to a new, empty table for subsequent audit records.
- The syslogs transaction log device – stores transaction logs.

When you configure for auditing, you must specify a separate device for the `syslogs` system table, which contains the transaction log. The `syslogs` table, which exists in every database, contains a log of transactions that are executed in the database.

Preinstallation for Auditing Devices

Determine the location of the raw devices you need for the `sybsecurity`, `syslogs`, and `sysaudits` table devices.

Configure your system with the minimum number of auditing devices you require—you must configure at least three. You can add more auditing devices later using **sp_addaudittable**. For information, see the *Reference Manual: Procedures*.

Sybase recommends that you:

- Install auditing tables and devices in a one-to-one ratio. Tables that share the same device will share the same upper threshold limit. These tables cannot be used sequentially when a device fills up, because they both reside on the same device.
- Install each auditing table on its own device. This enables you to set up a smoothly running auditing system with no loss of auditing records.

  With two auditing tables, when one fills up, you can switch to the other. With a third auditing table, if one device fails, the system security officer can install a new threshold procedure that changes the device rotation to skip the broken device until the device is repaired.
- Make the device larger than the table. When you use only three auditing tables and devices, the size of the table and the size of the device can be similar, because you can obtain more auditing capacity by adding more auditing tables and devices. When you are working toward the upper table and device limit (six to eight), you may want to make the device considerably larger than the table. You can then later expand the table size towards the upper size of the device when you need a larger auditing capacity is desired, and no additional devices.

Installing Auditing

By default, the Adaptive Server auditing feature is not installed.

For more information about auditing, see the *Security Administration Guide*.

1. Open a Command Prompt window.
2. Start the **isql** program as user "sa":

   ```
   isql -Usa -Ppassword -Sserver_name
   ```
3. Determine the next available device number to use for the auditing device.

   For the auditing database itself:

```
1> declare @devno int
2> select @devno = max(low/16777216)+1 from sysdevices
3> disk init
4> name = "auditdev",
5> physname = "%SYBASE%\data\sybaud.dat",
6> vdevno = @devno,
7> size = 5120
8> go
```

For the auditing database log:

```
1> declare @devno int
2> select @devno = max(low/16777216)+1 from sysdevices
3> disk init
4> name = "auditlogdev",
5> physname = "%SYBASE%\data\sybaudlg.dat",
6> vdevno = @devno,
7> size = 1024
8> go
```

4. At the **isql** prompt, use the **disk init** command to create the auditing devices.
5. Create the auditing database:

   ```
   1> create database sybsecurity on auditdev
   2> log on auditlogdev
   3> go
   ```

6. Exit **isql**:

   ```
   exit
   ```

7. Change to the `scripts` directory:

   ```
   cd %SYBASE%\ASE-15_0\scripts
   ```

8. Set the DSQUERY environment variable:

   ```
   set DSQUERY = server_name
   ```

9. Start the **isql** program as user “sa” with the **instsecu** script as the input file:

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

10. Restart Adaptive Server.

After auditing is installed, no auditing occurs until a system administrator or system security officer enables auditing with the auditing system procedures. See the *Security Administration Guide*.

CHAPTER 18 Install Online Help for Transact-SQL Syntax

The %SYBASE%\%SYBASE_ASE%\scripts directory contains scripts for installing the syntax help database, sybsyntax.

You can install any of these scripts, depending on the need for Sybase information on your server. The first script you execute creates the sybsyntax database and the needed tables and indexes. Any scripts that you execute after the first one add to the existing information in the database. If you reexecute a script, any previously installed rows of information are deleted from the table in the database and then reinstalled.

You can retrieve this data using **sp_syntax**. For more information on **sp_syntax**, see the *Reference Manual: Procedures*.

All Adaptive Server installations include the **ins_syn_sql** script, which includes syntax information for Transact-SQL, the system procedures, and Sybase utilities. Executing this script installs the SQL portion of the sybsyntax database.

Default Device for the sybsyntax Database

The sybsyntax database requires device space that is at least as large as the model database. By default, the sybsyntax installation scripts install the sybsyntax database on the device that is designated as the default database device.

If you have not used **sp_diskdefault** to change the status of the master device (which is installed as the default disk) or to specify another default device, the scripts install sybsyntax on the master device. Sybase recommends that you do not use this configuration, because sybsyntax uses valuable space, that is best left available for future expansion of the master database.

To avoid installing sybsyntax on the master device, do one of:

- Use **sp_diskdefault** to specify a default device other than the master device. For information about **sp_diskdefault**, see the *Reference Manual: Procedures*.
- Modify each sybsyntax installation script that you plan to execute to specify a different device.

Installing sybsyntax

The `sybsyntax` installation script installs the database and the necessary tables and indexes.

1. Determine the type (raw partition, logical volume, operating system file, and so on) and location of the device where you plan to store the `sybsyntax` database.
2. Make a copy of the original script. Be sure you can access this copy, in case you experience problems with the edited script.
3. Use a text editor to edit the script, if necessary, to change the default device from the master device to the device created in step 1.
   - Comment out this section, which specifies the default device:

     ```
     /* create the database, if it does not exist */
      if not exists (select name from sysdatabases
      where name = "sybsyntax")
      begin
          /* create the sybsyntax table if it doesn't exist */
          /* is the space left on the default database
          devices > size of model? */
          if (select sum (high-low +1) from sysdevices where status
          & 1 = 1) - (select sum(size) from sysusages, sysdevices
              where vstart >= sysdevices.low
              and vstart <= sysdevices.high
              and sysdevices.status &1 = 1) >
              (select sum(sysusages.size) from sysusages
              where dbid = 3)
          begin
              create database sybsyntax
          end
          else
          begin
              print "There is not enough room on the default
              devices to create the sybsyntax database."
          return
          end
      end
     ```

     where *device_name* is the name of the device on which to install `sybsyntax`.
   - After you have commented out this entire section, add this line:

     ```
     create database sybsyntax on device_name
     ```
4. Execute the script:

   ```
   isql -Usa -Ppassword -Sservername < %SYBASE%\%SYBASE_ASE%\scripts
   \ins_syn_sql
   ```

   where *sa* is the user ID of the system administrator, *password* is the system administrator's password, and *servername* is the Adaptive Server where you plan to install the database.

   If you have set the DSQUERY environment variable to *servername*, you can replace the server name with DSQUERY:

```
isql -Usa -Ppassword -S$DSQUERY < %SYBASE%\%SYBASE_ASE%\scripts
\Sins_syn_sql
```

5. To ensure that you have installed the `sybsyntax` database and that it is working correctly, use **isql** to log in to the server on which you installed the database, and execute **sp_syntax**:

   ```
   isql -Usa -Ppassword -Sservername

   1> sp_syntax "select"
   2> go
   ```

   Adaptive Server displays a list of commands that contain the word or word fragment "select".

CHAPTER 19 Troubleshoot Network Connections

Net-Library enables clients and Adaptive Servers to interact over a network. If the Net-Library software is not functioning properly, the client/server environment is also affected.

Use the Server Ping utility in the Directory Services Editor (**dsedit**) to get information about Adaptive Servers on a network, including both successful connections and failed connection attempts. .

Running Server Ping

Use Server Ping to identify more than one server in the `sql.ini` file from many.

You do not need to have a valid user name on Adaptive Server to run Server Ping.

1. Start **dsedit**.
2. Select the directory service to open, and click **OK**.
3. Select the name of the server to test.

   The server information you see depends upon the specific Net-Library driver that you have installed.
4. Select **Server Object/Server 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.

Troubleshoot Connection Failures

When a client application fails to connect to a server, you can test the application for diagnostic purposes. Messages from Server Ping 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.

When Server Ping reports an unsuccessful connection, verify that:

- 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 the *Installation Guide*).
- 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.
- The connection information in your client's network configuration file is correct. See the Net-Library documentation for your client.
- The format of the connection information is correct for the network protocol.

Using Returned Messages to Diagnose a Failure

Review Server Ping messages to determine the point at which the ping failed.

Troubleshooting a Connection Failure to Adaptive Server

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.

1. Verify that the server is running.
2. Make sure your networking software and hardware are properly configured.
3. See whether the network has generated any messages.
4. Verify that the connection information is correct for your network protocol and that connection entries are formatted correctly.

Failure to Load Net-Library DLLs

Server Ping displays a message when it cannot load the Net-Library DLL. Verify that the directory containing Net-Library DLL is included in the PATH environment variable.

Troubleshooting Failure of Other Applications

When Server Ping reports no errors, but your other applications fail to run, verify your connection settings.

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 can be successful even if 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, collect pertinent information before you call Sybase Technical Support

When you call Sybase Technical Support, have:

- 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.

CHAPTER 20 Adaptive Server Registry Keys

The Windows operating system stores configuration information in a tree-structured file called the Registry.

When you install Adaptive Server for Windows, the installation program and Server Config write configuration information to several branches, called *keys*, in the Windows Registry.

In some cases, you may be able to change Registry changes to configure Adaptive Server features. However, you can seriously impair your Windows system if you make incorrect changes to the Registry.

Warning! Do not modify key values in the Registry unless you are an experienced Windows administrator, and you are familiar with the **regedt32** utility. See your system Windows documentation for information about using **regedt32**.

\SOFTWARE\SYBASE\Server\server_name

Registry values for the \SOFTWARE\SYBASE\Server\server_name key that appears under HKEY_LOCAL_MACHINE in the Registry.

HKEY_LOCAL_MACHINE\SOFTWARE\SYBASE\Server\server_name			
Key Name	**Type**	**Default**	**Description**
DefaultDomain	REG_SZ	None	The default domain for mapping Windows user names to Adaptive Server logins
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

HKEY_LOCAL_MACHINE\SOFTWARE\SYBASE\Server\server_name			
Key Name	**Type**	**Default**	**Description**
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	SQLServ-er	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

\SOFTWARE\SYBASE\SQLServer\server_name\parameter

Registry values for the \SOFTWARE\SYBASE\SQLServer\server_name\parameter key that appears under HKEY_LOCAL_MACHINE in the Registry.

HKEY_LOCAL_MACHINE\SOFTWARE\SYBASE\SQLServer\server_name \parameters			
Key Name	**Type**	**Default**	**Description**
Arg0	REG_SZ	`-dD:\sybase \ASE-15_0\ 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	`-ed:\sybase \ASE-15_0\in-stall\ 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

HKEY_LOCAL_MACHINE\SOFTWARE\SYBASE\SQLServer\server_name \parameters			
Key Name	**Type**	**Default**	**Description**
Arg5	REG-SZ	`-Nd:\sybase \ASE-15_0\sysam\ <srv_name>.prop- erties`	Location and name of license cache file

\SOFTWARE\SYBASE\SQLServer

Registry values for the \SOFTWARE\SYBASE\SQLServer key that appears under HKEY_LOCAL_MACHINE in the Registry.

HKEY_LOCAL_MACHINE\SOFTWARE\SYBASE\SQLServer			
Key Name	**Type**	**Default**	**Description**
CurrentVersion	REG_SZ	Windows 15.0	The version number for the Adaptive Server software installed on the computer.
DefaultBackup-Server	REG_SZ	*server_name*_BS	The name of the default Backup Server.
DSEVNTLOG	REG_SZ	LocalSystem	The destination machine for logging messages to the Windows 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	15.0	The version number of the Adaptive Server.

\SYSTEM\CurrentControlSet\Services \SYBSQL_server_name

Registry values for the \SYSTEM\CurrentControlSet\Services\SYBSQL_server_name key that appears under HKEY_LOCAL_MACHINE in the Registry.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \SYBSQL_server_name			
Key Name	**Type**	**Default**	**Description**
Display-Name	REG_SZ	Sybase SQL Server_*server_name*	The Adaptive Server name used in the Services list under Control Panel
ErrorCon-trol	REG_DWORD	0x1	For system use only
ImagePath	REG_EX-PAND_SZ	`D:\Sybase \ASE-15_0\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
Type	REG_DWORD	0x10	For system use only

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U