New Features Bulletin Adaptive Server® Enterprise 15.0.2 ESD #2

Document ID: DC00775-01-1502-01

Last revised: December 11, 2007

Accessing current information

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

❖ **Accessing new features bulletins at the Sybase Product Manuals Web site**

1 Go to Product Manuals at http://www.sybase.com/support/manuals/.

Copyright 1987-2007 by Sybase, Inc. All rights reserved. Sybase trademarks can be viewed at the Sybase trademarks page at http://www.sybase.com/detail?id=1011207. Sybase and the marks listed are trademarks of Sybase, Inc. ® indicates registration in the United States of America. Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Unicode and the Unicode Logo are registered trademarks of Unicode, Inc. All other company and product names mentioned may be trademarks of the respective companies with which they are associated.

2 Select a product and language and click Go.

3 Select a product version from the Document Set list.

4 From the list of individual documents, select the link to the bulletin. You can either download the PDF version or browse the document online.

Configuring LDAPS

User authentication for Lightweight Directory Access Protocol (LDAP) now supports the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol, as described in the *Adaptive Server 15.0.2 New Features Guide*, for Solaris 32-bit, 64-bit, Linux AMD 64, and Linux 32-bit on Intel platforms. This feature provides secure data transmission between Adaptive Server and an LDAP server, and is called LDAPS.

LDAPS provides data transmitted between Adaptive Server and LDAPS servers.

❖ **Configure an LDAPS connection**

1 Make sure that all trusted root certificates are located in the same file.

After you define the trusted servers, Adaptive Server configures a secure connection, where *servername* is the name of the current Adaptive Server. If you:

- Have defined *$SYBASE_CERTDIR*, Adaptive Server loads certificates from *$SYBASE_CERTDIR/servername.txt* (for UNIX) or *%SYBASE_CERTDIR%\servername.txt* (for Windows).
- Have not defined *$SYBASE_CERTDIR* Adaptive Server loads certificates from *$SYBASE/$SYBASE_ASE/certificates/servername.txt* (for UNIX) or *%SYBASE%\%SYBASE_ASE%\certificates\servername.txt* (for Windows).

2 Restart Adaptive Server to change the trusted root certificate file.

3 Use sp_ldapadmin, specifying *ldaps://* URLs instead of *ldap://* URLs, to establish a secure connection to a secure port of the LDAPS server.

4 Establish a TLS session over a plain TCP connection:

```
sp_ldapadmin 'starttls_on_primary', {true | false}
```

or

sp_ldapadmin 'starttls_on_secondary', {*true* | *false*}

Note LDAPS connections do not have a connect timeout option; if the LDAP server stops responding, all login connections also stop responding.

Dumping QP metrics for ad hoc statements

When you enable the statement cache, the QP metrics for ad hoc statements using the statement cache are not instantly dumped into the sysquerymetrics system catalog. Instead, the QP metrics of the respective ad hoc statements are dumped when the statement is flushed out of the statement cache, or by commands such as sp_metrics 'flush' and dbcc purgesqlcache.

You can revert this default behavior by using trace flag T7724.

Receiving e-mail notifications about SySAM licensing

When you configure Adaptive Server to send an e-mail notice of SySAM licensing failures, the e-mail messages do not contain HELO tokens, which some SMTP mail servers require to process messages correctly. If your SMTP server requires such a HELO token, append the "email.helo.fqdn" property to the SySAM property file. The property value should be the fully qualified domain name, such as:

```
email.helo.fqdn=sybase.com
```

The SySAM properties file is located in the *$SYBASE/ASE-15_0/sysam* directory and is named *servername.properties*, where *servername* is the name of your server.

Increased support for exporting set options from a login trigger

Adaptive Server version 12.5.4 enabled options set inside login triggers to remain valid for the entire user session, and supported a list of exportable options. Adaptive Server 15.0.2 ESD #2 expands the list to include the following:

addend_union_all	merge_union_distinct	showcounters
auto_query_tuning	multi_gt_store_index	showelimination
basic_optimization	nary_nl_join	showexecio
bushy_space_search	nl_join	showfinalplan
distinct_hashing	opportunistic_distinct	showhistograms
distinct_sorted	opportunistic_grouping	showliocosting
distinct_sorting	optgoal	showlogprops
group_hashing	opttimeout	showlop
group_inserting	order_sorting	showmanagers
group_sorted	parallel_query	shownostats
hash_union_distinct	query_tuning_mem_limit	showparallel
index_intersection	query_tuning_time_limit	showpiocosting
index_union	replicated_partitioning	showpllcosting
hash_join	showabstractplan	showsearchengine
merge_join	showbestplan	store_index
merge_union_all	showcodegen	streaming_sort

For the list of options already supported, see the *Adaptive Server Enterprise New Features Guide* for version 12.5.4.

New and changed commands, functions, stored procedures, and utilities

This section describes new and changed commands, built-in functions, stored procedures, and utilities for Adaptive Server 15.0.2 ESD #2. See these documents for general information about these topics:

- Commands – *Reference Manual: Commands*
- Functions – *Reference Manual: Functions*

- Stored procedures – *Reference Manual: Procedures*
- Utilities – *Utility Guide*

New *create manifest file* command

The manifest file is the binary file that describes the databases that are present on a set of database devices. It can be created only if the set of databases that occupy those devices are isolated, and self-contained on those devices.

Use the create manifest file command to create a manifest file, which you need to run the quiesce database command for mounting and unmounting databases.

For more information, see "Using mount and unmount commands" in the "Backup and Recovery Plan" chapter of *System Administration Guide, Volume 2*.

Description

Creates a manifest file for one or more databases.

Syntax

create manifest file *database_list* to *manifest_file_name*

Parameters

- *database_list* – is the list of databases for which you are creating a manifest file.
- *manifest_file_name* – is the name of the manifest file you are creating. Enclose full path names in quotes.

Examples

Example 1 Creates a manifest file for the database big_database in the current directory:

```
create manifest file big_database to big_database_manifest
```

Example 2 Creates a manifest file for the databases big_database, medium_database, and small_database:

```
create manifest file big_database, medium_database, small_database to
    '/sybase/data/database_manifest'
```

Usage

- You cannot run create manifest file within a transaction.
- You cannot include system databases in the *database_list*.
- You cannot run create manifest file in a high availability system that is in a transient (failover or failback) state.
- You cannot include a database in the *database_list* that resides on a disk that is shared by another database that is not included in the manifest file list.
- You cannot create a manifest file for an archived database.

Permissions	You must have the sa_role or oper_role to run create manifest file.
Auditing	create manifest file is audited by audit event number 116.

Change in the maximum nesting level of stored procedure/trigger execution

The maximum nesting level of stored procedure/trigger execution has increased from 16 to 50.

Changes to *sp_configure 'histogram tuning factor'* parameter

Adaptive Server 15.0.2 ESD #2 introduces a change to the 'histogram tuning factor' parameter in sp_configure. This parameter controls the number of steps Adaptive Server analyzes per histogram for update statistics, update index statistics, update all statistics, and create index.

If you set the 'histogram tuning factor' configuration parameter to its default value of 20 and a large number of steps are requested for the histogram, then the actual step count used for the histogram is limited to:

min (max (400, requested_steps), histogram_tuning_factor * requested_steps)

This is designed to reduce the procedure cache usage.

Changes to *sp_modifylogin* stored procedure

The sp_modifylogin stored procedure has a new value that lets you clear the previous setting for an option you set for a specific user. The value is 'clear' and uses this syntax for the "passwd expiration", "min passwd length", and "max failed_logins" options:

sp_modifylogin *loginame*, *option*, 'clear'

Example

In this example, sp_modifylogin was used to set to the password expiration for a user named “John” to expire in 30 days, even though the system default for password expiration is 90 days:

```
1> sp_modifylogin 'John', 'passwd expiration', 30
2> go
```

Using 'clear', we can now remove this 30-day password expiration on John:

```
1> sp_modifylogin 'John', 'passwd expiration', 'clear'
2> go
```

If John's password expiration setting had been changed previously, executing the command returns a message similar to the following, and John's password expiration returns to being the same as the system default:

```
The login-specific 'passwd expiration' attribute has
been removed.
```

If John's password expiration was not manually changed from the system default, executing the command returns a message such as:

```
There is no login-specific 'passwd expiration'
attribute set for this user.
```

This means that your sp_modifylogin changed nothing, and John's password expiration is still the same as the system default.

Changes to *ddlgen* utility

When you issue the ddlgen utility in a UNIX command line environment, other users on that UNIX machine can see your ddlgen command—including its password—if they issue the ps process management command, which shows the status of processes that are running on that machine.

Adaptive Server 15.0.2 ESD #2 includes a new ddlgen -P password parameter option that lets you invoke ddlgen from a script so that the password is hidden from other users.

To do this, include the string "pwd" in the -P parameter. This acts as a pseudo-password, while you supply the actual password in the next line of the script:

```
ddlgen -Ulogin -Ppwd -Sserver:port -Ttype -Nname << END
$PSWD
END
```

The actual ddlgen password string is hidden in the $PSWD environment variable.

If you prefer to keep your password in a file, replace $PSWD with 'cat *filename*', where *filename* is the location of your password file. For example:

```
ddlgen -Ulogin -Ppwd -Sserver:port -Ttype -Nname << END
'cat filename'
END
```

For more information about ddlgen, see the ddlgen reference pages in the *Utility Guide*.

New and changed system tables

This section describes new and changed system tables for Adaptive Server 15.0.2 ESD #2. For more information about system tables, see *Reference Manual: Tables*.

monEngine

The monEngine table, which provides statistics regarding Adaptive Server engines, has a new column called Max outstanding IOs. Max outstanding IOs provides information on IO queue sizes on a per-engine basis.

```
1> select EngineNumber, MaxOutstandingIOs
       from monEngine
2> go

 EngineNumber MaxOutstandingIOs
 ------------ -----------------
            0                 6
            1                 0

(2 rows affected)
```

monOpenDatabases

The monOpenDatabases Monitoring and Diagnostic (MDA) table, which provides state and statistical information pertaining to databases that are currently in use, has these new columns:

Column name	Datatype	Description
LastCheckpointTime	datetime	The date and time that the last checkpoint started for the database. If no checkpoint occurs, the value is NULL.

Column name	Datatype	Description
LastTranLogDumpTime	datetime	The date and time that the last dump transaction started for the database. If: • There is no dump transaction, the value is NULL. • The transaction is dumped using the truncate_only or no_log clause, the time is not updated.

Note The original BackupStartTime column is updated only when a database is dumped.