SYBASE®
An SAP® Company

New Features Guide

Adaptive Server® Enterprise 15.7 SP50

DOCUMENT ID: DC00641-01-157050-01
LAST REVISED: July 2013

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

Contents

CHAPTER 1: Remote Dump Host Control 1

CHAPTER 2: Job Scheduler Enhancements 3

Job Scheduler Automatic Restart 3
Logging of Job Scheduler and Job Execution Errors 4
Configuration Parameter for Core Dumps 5

CHAPTER 1 Remote Dump Host Control

Backup Server introduces a remote access control feature that prevents remote dumps and loads, and execution of remote procedure calls (RPCs) from any client or server that is running on unauthorized servers.

Access Control File

Authorization to dump to, or load from, Backup Server is achieved by including the authorized hosts in the `hosts.allow` file. The default name of the file is `hosts.allow`, which is by default located in `$SYBASE`. You can change the location and file name using:

```
backupserver -h full_path_name/hosts.allow
```

When you start Backup Server, the location of the file is shown in the error log. For example:

```
Backup Server: 1.88.1.1: The hosts authentication file used by
the backup server is '/remote/myServer/ase157x/SMP/release/
hosts.allow'.
```

If you do not specify a file, `$SYBASE/hosts.allow` is used. If the location of the file is a relative path, the path is replaced by the absolute path using the directory in which the Backup Server has been started. For example, if you start Backup Server from `/usr/u/myServer` and Backup Server is started with:

```
backupserver -h./myhosts.allow
```

The error log shows:

```
Backup Server: 1.88.1.1: The hosts authentication file used by
the backup server is '/usr/u/myServer/./myhosts.allow'.
```

If the file `hosts.allow` does not exist, dump or load commands, or remote procedures, fail.

Note: Local dumps are not affected by this feature.

File Content

The format for `hosts.allow` is:

```
host_name_running_backupserver [ \t*][,][ \t*] host_name_trying_to_connect

host_name_running_backupserver:
hostname | hostname.domain | ipv4 address | ipv6 address

host_name_trying_to_connect:
hostname | hostname.domain | ipv4 address | ipv6 address |+

The '+' sign can be used as a wildcard to allow remote
```

```
dumps to, or loads from, any Backup Server running on
the specified host.
```

```
Example:
# Example of hosts.allow file
# Development machine imetsol1 allows access from everywhere
imetsol1 +

# Group development machine marslinuxX allow access from other
# marslinuxX machines only
marslinux1 marslinux2
marslinux1 marslinux3
marslinux2 marslinux1
marslinux2 marslinux3
marslinux3 marslinux1
marslinux3 marslinux2
```

Permissions

The recommended file permission for UNIX is no greater than `640`. For Windows, ensure that only authorized users are granted access to the file.

Error and Warning Messages

- On UNIX, if permission levels are set lower than `640`, you see a warning similar to:
  ```
  Backup Server: 1.86.1.1: Warning: The file './hosts.allow'
  has an unsafe permission mask 0664. The recommended value is
  0640.
  ```
- On Windows, if you have not established permissions, or if access is granted to everyone, you see a warning similar to:
  ```
  Backup Server: 1.87.1.1: Warning: The file './hosts.allow'
  either has no access control or one of the entries allows
  access to everyone. It is recommended that only the owner
  has permission to access the file.
  ```
- If you attempt to load to, or dump from, a remote Backup Server that does not have the appropriate access control record, you see error:
  ```
  Backup Server: 5.16.2.2: Client-Library error: Error number
  44, Layer 4, Origin 1, Severity 4: ct_connect(): protocol
  specific layer: external error: The attempt to connect to
  the server failed. Backup Server: 5.3.2.1: Cannot open a
  connection to the slave site 'REMOTE_BS'. Start the remote
  Backup Server if it is not running.
  ```
- If you attempt to execute an RPC on a remote Backup Server that does not have the appropriate access control record, you see error:
  ```
  Msg 7221, Level 14, State 2:
  Server 's', Line 1:
  Login to site 'REMOTE_BS' failed.
  ```

CHAPTER 2 Job Scheduler Enhancements

Adaptive Server® version 15.7 SP50 provides Job Scheduler enhancements, such as an automatic restart feature and a new configuration parameter for controlling core dumps.

Job Scheduler Automatic Restart

Adaptive Server introduces a Job Scheduler automatic restart feature that is implemented during various states of Job Scheduler Agent (JS Agent) and Job Scheduler Task (JS Task).

Automatic restart occurs when:

- JS Agent is in an inconsistent state but still running.
  This may be as a result of the connection in a pool stopping, or if the target server has stopped while collecting results.
  In this situation, both the JS Task and JS Agent are shut down and restarted.
- JS Task is in an inconsistent state and is going to shut down Job Scheduler.
  This may be as a result of an inconsistency detected in Job Scheduler tables; alternatively, it may be due to incorrect or missing job callouts.
  In this situation, both the JS Task and JS Agent are shut down and restarted.
- JS Agent has stopped running.
  This may be as a result of JS Agent hitting a fatal signal, JS Agent shutting down due to inconsistency detected in its operation, or an external event, such as the killing of a JS Agent process.
  JS Task periodically monitors JS Agent health. If it finds that the JS Agent has stopped, it will restart the JS Agent.
- JS Task unexpectedly stops running.
  In this situation, you must manually restart Adaptive Server. A new JS Task aborts the existing JS Agent, if any, and starts a new JS Agent.

New Configuration Options

Table 1. max js restart attempts

Default value	3
Range of values	0 – 10
Status	Dynamic

Display level	10
Required role	System administrator
Configuration group	SQL Server Administration

Restricts the number of restart attempts and prevents the Job Scheduler restart feature from going into an infinite loop. The value 0 indicates that the Job Scheduler Auto restart feature is disabled.

Table 2. enable js restart logging

Default value	0 (Job Scheduler logging disabled)
Range of values	0, 1
Status	Dynamic
Display level	10
Required role	System administrator
Configuration group	SQL Server Administration

Enables or disables diagnostics logging after the restart of Job Scheduler.

Table 3. js heartbeat interval

Default value	1
Range of values	1 – 1440
Status	Dynamic
Display level	10
Required role	System administrator
Configuration group	SQL Server Administration

The intervals between two JS Agent heartbeat checks, in minutes.

Logging of Job Scheduler and Job Execution Errors

Job Scheduler errors and job execution errors are logged to the Adaptive Server, JS Agent log by default. Additional diagnostics information can be enabled using the existing 3641 trace flag.

Configuration Parameter for Core Dumps

You can use the `disable jsagent core dump` configuration parameter to enable or disable JS Agent core dumps.

Note: Having JS Agent core dumps enabled allows you to diagnose JS Agent crash issues. Disabling core dumps for JS Agent is not recommended.

The JS Agent can generate core dumps files when a fatal signal (or an exception on Windows) is encountered. This can be useful when diagnosing Job Scheduler issues. The default location for a core dump is determined by the environment variable `JSA_CORE_PATH`.

- If `JSA_CORE_PATH` is not set, or you do not have write permission to the set path, the `$SYBASE/$SYBASE_ASE/install` path is used.
- If `$SYBASE` or `$SYBASE_ASE` is not set, then directory from where the JS Agent process was started is used. $SYBASE path is used for Windows.

Note: For the AIX platform, the core file is generated in the directory from where the JS Agent process was started.

New Configuration Option

Table 4. disable jsagent core dump

Default value	0
Range of values	0 , 1
Status	Dynamic
Display level	10
Required role	System administrator
Configuration group	SQL Server Administration

Disables JS Agent core dump for all platforms. When off (0), the core dump for JS Agent is enabled during signal handling. Setting `disable jsagent core dump` to on (1) disables core dumps and is not recommended.