

Enable the Pseudo Random Number Generator on IBM i to support SSL

Issue

Some SSL operations need the ability to generate random numbers. Zend provides a PRNGD (Pseudo Random Number Generator Daemon) to fill this requirement, but it does not run by default. This article tells how to set it up to run.

Environment

Zend Server 6 or higher, running on any supported version of IBM i

Note: This document is using the current version of Zend Server (Zend Server 2021.x)

If you are running Zend Server 9.1.x - 2019.x, please replace all references of ZENDPHP74 or zendph74 with **ZENDPHP7 and zendphp7**

If you are running Zend Server 6 - 8.5.x, please replace all references of ZENDPHP74 or zendph74 with **ZENDSVR6 and zendsvr6**

If you are running Zend Server 5.x, please replace all references to ZENDPHP74 or zendphp74 with **ZENDSVR and zendsvr**

Resolution

To set the PRNGD to run whenever the ZENDPHP74 subsystem is started, configure it in the Autostart Job Settings.

Note that the menus were changed for version 8.5 of Zend Server, so the menus you have will depend on your version of Zend Server.

From the command line:

GO ZENDPHP74/ZSMENU

For version 8.5 and higher:

Use menu option "80. Configurations". Then use menu option "3. Autostart Job Settings".

For prior versions:

Use menu option "10. Autostart Job Settings"

The Autostart job settings will look something like this:

Type choices, press Enter.

```
Monitor daemon (Y/N) . . . . . > Y
Java Bridge daemon (Y/N) . . . . > N
Job Queue daemon (Y/N) . . . . . > Y
Deployment daemon (Y/N) . . . . . > Y
Prngd daemon (Y/N) . . . . . > N
Zend Server Daemon (Y/N) . . . . > Y
```

Find "Prngd daemon" on the list, and set it to 'Y', like this:

Type choices, press Enter.

```
Monitor daemon (Y/N) . . . . . > Y
Java Bridge daemon (Y/N) . . . . > N
Job Queue daemon (Y/N) . . . . . > Y
Deployment daemon (Y/N) . . . . . > Y
Prngd daemon (Y/N) . . . . . > Y
Zend Server Daemon (Y/N) . . . . > Y
```

Settings you have for the other daemons may be different from what you see here. This is OK. Press enter to save the changes.

Note:

Some older versions of Zend Server will [set the wrong data area value for the Zend Server Daemon](#) and set the correct value off. This can be corrected by running the following command:
CHGDTAARA DTAARA(ZENDPHP74/ZAUTOJOB (7 1)) VALUE('1')

The next time the ZENDPHP74 subsystem is restarted, use wrkactjob to verify that the PRNGD is started. From the command line:

```
wrkactjob sbs(zendphp74)
```

If the PRNGD daemon is active, you should see these two jobs:

ZS_STR_PRN	QTMHHTTP	BCH	.0	PGM-prngd	THDW
ZS_STR_PRN	QTMHHTTP	BCI	.0	PGM-prngd	SELW

You don't have to wait for your next restart to run the PRNGD. Like all the daemons, the PRNGD has its own menu to start and stop the job. From the command line:

```
go zendphp74/zspmenu
```

Use option "1. Start PRNGD (ZS_STR_PRN) job". You can use the same wrkactjob command as noted above to verify that the ZS_STR_PRN jobs are active.

Note: For PHP 5.6 and higher, you will also need to set up a Trusted Certificate Authority.

[Add a trusted certificate authority to IBM i for PHP 5.6](#)