Problem Determination Tools for z/OS Common
Component for z/OS V1R6

Addenda to Problem Determination Tools for z/OS Common Component V1R6 documentation

Contents

About this document

This document provides details of all the APAR service fixes that impact upon documentation for IBM Problem Determination Tools for z/OS Common Component for z/OS Version 1.6, since the most recent edition of the product manual. This edition is:

- Customization Guide and User Guide (SC19-3690-02) - Third Edition

The Addendum document is divided into two parts:

- **Part 1: PTF/APAR documentation changes**

  This section lists the changes to the Problem Determination Tools for z/OS Common Component Version 1 Release 6 documentation that are required to reflect new behavior resulting from the application of APAR fixes.

  The fixes are listed by PTF number, in reverse date order, so that the most recently released fix appears at the beginning of the document. Each description shows:

  - The set of PTF numbers in the release
  - The date of the PTF release
  - The APARs included in the released fix
  - Details of those APAR changes that affect documentation
  - Page references for the manuals affected by the change

  Note:

  1. This document does NOT describe those APAR fixes that do not have an impact upon documentation.
  2. The enhancements and corrections described in this section are only available after applying the listed PTFs for the APAR.

- **Part 2: General documentation changes**

  This section describes enhancements, corrections and updates in the documentation for Problem Determination Tools for z/OS Common Component for z/OS Version 1 Release 6. These changes are not associated with PTF numbers, as they do not require the application of any code updates.

  The changes are in reverse date order. That is, the most recent documentation change appears at the beginning of the section.

The page numbers referenced in this document are the page numbers in the latest version of the relevant PDF. The page number refers to the start of the section or subsection.

There are no changes listed in this Addendum. At the moment, the -02 edition of the Customizationg Guide and User's Guide is up to date.

Part 1. PTF/APAR documentation changes

UI29686

Release Date: **28 July 2015**

This set of PTFs contains these APAR fixes:
- PI39498

PI39498

Initial problem description

1. No ability to select the minimum protocol for secured communications is available.

   For clients prior to 13.1.0.16 this prevents them from communicating with the server at UI26365.

Outline of solution

1. The common server has been updated in order to support setting of the minimum protocol to one of:
   - TLSv1
   - TLSv1.1
   - TLSv1.2

Documentation impact

This APAR requires changes to:
- Problem Determination Tools for z/OS Common Component Customization Guide and User Guide Version 1 Release 6 (SC19-3690-02)

Changes to the "Customization Guide and User Guide"

In Chapter 2 "Server overview" in the section "Configuration file keyword descriptions" (page 4), *change* the description for SSL_REQUIRED to the following:

SSL_REQUIRED=YES|TLSV1|TLSV1.1|TLSV1.2|NO (Optional, default is NO)

Determines whether SSL encrypted communications are mandatory for the server and the desired protocol level. SSL communications are achieved by utilising the System SSL APIs. The default protocol level is TLS V1.1 when YES is specified. Older clients (prior to common component client 13.1.0.16) require TLS V1.

To use TLS V1.2, clients must be at level 13.1.0.17 or later.

If SSL encryption is used, then the server uses a certificate stored in either a RACF keystore, when specified via the SSL_KEYRING keyword, or a GSKKYMAN managed key database and certificate for this server as specified in the SSL_CERT keyword or, if that keyword is omitted, at the WORKDIR specified location.

UI26365

Release Date: **31 March 2015**

This set of PTFs contains these APAR fixes:
- PI30882
- PI33925

PI30882

Initial problem description

1. No documentation exists for setting the cipher specification to be used by System SSL for common servers with SSL active.
2. Setting the cipher for System SSL is not propagated to the user session launched by the common server.

Outline of solution

1. The documentation update is provided below.
2. The common server has been modified in order to propagate the settings for environment variables GSK_V3_CIPHER_SPECS or GSK_V3_CIPHER_SPECS_EXPANDED to the launched user session. The sample server JCL and the Customisation Guide have been updated in order to show how to set environment variables used by System SSL to set the cipher specifications.

Documentation impact

This APAR requires changes to:
- Problem Determination Tools for z/OS Common Component Customization Guide and User Guide Version 1 Release 6 (SC19-3690-02)

Changes to the "Customization Guide and User Guide"

In Chapter 3 "Customizing the PDTCC Server" in the section "Setting SSL encrypted communications", *add* (page 8) the following:

If you wish to specify a cipher string for the System SSL component to use, you can do this by modifying the server JCL to specify an ENVAR(GSK_V3_CIPHER_SPECS=xx) or ENVAR(GSK_V3_CIPHER_SPECS_EXPANDED=xx) as required. The sample server JCL member IPVSRV1 includes an example format of the above.

PI33925

Initial problem description

Users may want to provide TIME and ACCOUNT settings for tasks launched by the common server.

Outline of solution

The common server has been modified in order to add support for configuration keywords:
- SPAWN_TIME=nnn - where nnn is the number of seconds of CPU TIME If this value is set too low, server extensions will fail to launch with return code 0BBA0425.

- SPAWN_ACCOUNT=accountingdata This data format is as per the _BPX_ACCT_DATA environmental variable.

Documentation impact

This APAR requires changes to:

- Problem Determination Tools for z/OS Common Component Customization Guide and User Guide Version 1 Release 6 (SC19-3690-02)

Changes to the "Customization Guide and User Guide"

In Chapter 2 "Server Overview" in the section "Configuration file keyword descriptions", *add* (page 5):

SPAWN_ACCT=*accountdata*

Allows specification of the account data used for the spawned address space. This is as per the _BPX_ACCT_DATA environment variable discussed in the z/OS UNIX System Services Planning manual.

SPAWN_TIME=*nn*

Allows specification of the CPU time limit, in seconds, used for the spawned address space.

UI20221

Release Date: **5 August 2014**

This set of PTFs contains these APAR fixes:
- PI15084

PI15084

Initial problem description

Many problems:
- Occasionally the server may excessively use CPU.
- Connections fail when the owner of the server contains '*' or '#' characters.
- Diagnosis output is difficult to collect when a server extension does not connect.
- When using SSL=NO, extensions may not receive all expected data.

Outline of solution

The following updates have been made:
- The server handles unexpected socket closures.
- The sample IPVMKDIR has been updated to handle userids containing special characters.
- Additional diagnostic messages have been added during server startup to confirm that pre-existing files in the WORKDIR are in the expected state. Also, the server now captures extension launch information for the JOBLOG and trace information until the extension has successfully established communications with the client.
- The internal API has been corrected.
- The server has been updated to support $VAR=value syntax in the configuration file. The sample IPVCONFG has been updated to include using substitution variables to reduce the need to repeat data set high level qualifiers.

None of the above changes require alteration of existing configurations.

Documentation impact

This APAR requires changes to:
- Problem Determination Tools for z/OS Common Component Customization Guide and User Guide Version 1 Release 6 (SC19-3690-02)

Changes to the "Customization Guide and User Guide"

In Chapter 3 "Customizing the PDTCC Server" in the section "Update sample IPVCONFG" (on page 9), *add*, after the existing bullet points:

The configuration file supports the setting and reference of substitution variables in the following form:

```
$VAR=value
```

For setting these variables, the above form may be specified before the first CONFIG statement, or otherwise between the CONFIG and SPAWN_PARMS_SECTION statements. If using concatenations for the CONFIG DD, the first CONFIG refers to the statements in the first of the concatenations.

In following statements in the configuration, occurences of '$VAR' are replaced by the 'value' specified. For example this could be used to represent high level qualifiers that are repeated in the configuration file. For example, set the value:

```
$IPVHLQ=SYS1.IPV
```

Then allow a reference in a following statement, such as:

```
SPAWN_STEPLIB=$IPVHLQ.SIPVMODA
```

The sample IPVCONFG makes use of this for high level qualifiers but it could also be used for other substitutions as desired.

Add the following sentence to the section "Create matching WORKDIR by running job IPVMKDIR" (page 9):

As the files in the workdir need to be owned by the servers userid, and the IPVMKDIR job issues the chown command, the file system they are mounted at needs to allow the changing of userid via the SETUID attribute.

Add the following messages to "Appendix A. Messages" (page 11).

IPV0041W Maximum user variables (500) reached when processing token %s, value %s in configuration %s

Explanation: The limit of substitution values has been reached.

System action: The server attempts to continue, however the configurations may be unusable.

User response: Examine the number of $token=value pairs present in the configuration file and reduce to less than 500.

IPV0042W Unable to stat file %s.

Explanation: The server is unable to check the configuration launch file entry.

System action: The server attempts to continue, however this launch configuration will be unusable.

User response: Examine the file path and ensure setup was completed correctly. Most likely the file or directory path is not owned or correctly permitted in order for this server instance to access the named file. The WORKDIR configuration step of installation needs to be checked and rerun.

IPV0043W Not owner of launch file %s.

Explanation: The server is not the owner of a configuration launch file entry.

System action: The server attempts to continue, however this launch configuration will be unusable.

User response: Examine the file path and ensure setup was completed correctly. Correct the condition by ensuring that the file owner is updated to the userid of the server. The file system that the file is mounted on needs to allow SETUID for the owner to be changed with the chmod command.

IPV0044W Launch file %s is not marked as sticky.

Explanation: A configuration launch file has not been created correctly.

System action: The server attempts to continue, however this launch configuration will be unusable.

User response: Examine the file path and WORKDIR location. If the WORKDIR is correct, the installation configuration step for the WORKDIR may need to be rerun.

UI17444

Release Date: **1 May 2013**

This set of PTFs contains these APAR fixes:
- PI14699

PI14699

Initial problem description
The common server does not provide an option to enable using a SAF keyring for the servers certificate and key.

Outline of solution
The common server has been updated in order to accept a new configuration keyword SSL_KEYRING which provides the name of the keyring to be used.

As the keyring is shared with the connecting users, the name should be specified in userid/ringname format. Userids (or groups) that are allowed to access the server need to be permitted UPDATE access to the profile IRR.DIGTCERT.LISTRING and also CONTROL access to IRR.DIGTCERT.GENCERT.

Documentation impact
This APAR requires changes to:
- Problem Determination Tools for z/OS Common Component Customization Guide and User Guide Version 1 Release 6 (SC19-3690-02)

Changes to the "Customization Guide and User Guide"

In Chapter 2 "Server Overview" in the section "Configuration file keyword descriptions", *add* (page 5):

SSL_KEYRING=userid/keyring
If SSL is being used for the server, provides the userid and keyring name for a certificate being held in a SAF keyring. The userid should match the ID used when creating the keyring.

In Chapter 3 "Customizing the PDTCC server", in the section "Setting SSL encrypted communications" on page 8, before the paragraph beginning "If you are using ICSF" *add*:

If using a SAF keyring, uncomment and modify the SSL_KEYRING line. The SSL_LABEL line should also be uncommented and modified if the certificate you generate does not have a label of 'PDTCC Server Certificate'.

For use of a certificate in a keyring, the userid of the server task or job, as well as the userids connecting to the server need to be permitted UPDATE access to the IRR.DIGTCERT.LISTING facility and CONTROL access to the IRR.DIGCERT.GENCERT facility in order to share the certificate amongst users of the common server.

For RACF users, a keyring and certificate could be created by the following example commands:

```
RACDCERT ID(IPVSRV) ADDRING(RINGA)
RACDCERT GENCERT SITE SIZE(1024)           -
         SUBJECTSDN(                       -
           CN('Common Server')             -
           OU('ADL')                       -
           O('ADL')                        -
           C('AU'))                        -
 WITHLABEL('PDTCC Server Certificate')
RACDCERT ID(IPVSRV)                                       -
         CONNECT(SITE LABEL('PDTCC Server Certificate')   -
         RING(RINGA) USAGE(PERSONAL)                      -
         DEFAULT)
SETR RACL REFR(DIGTCERT)
```

Note in the above that the userid IPVSRV is used for the userid of the common server task.

Updating the server config to include SSL_KEYRING=IPVSRV/RINGA would use the above generated certificate. These commands serve as a working example only and should be updated as desired to match your needs. RACDCERT commands are documented in the z/OS Security Server RACF Command Language Reference.

Part 2. General documentation changes

This section describes enhancements and updates in the documentation for Problem Determination Tools for z/OS Common Component for z/OS Version 1 Release 6. These changes are not associated with individual APAR or PTF numbers, as they do not require the application of any code updates.

The changes are grouped by manual and listed within each section in reverse date order. That is, the most recent documentation change appears at the beginning of each manual section.

There are no general documentation changes.

Index

Printed in USA