IBM Tivoli Key Lifecycle Manager Version 1.0
z/OS Fix Pack 4 README

Abstract

Readme documentation for IBM® Tivoli® Key Lifecycle Manager for z/OS, Version 1.0 Fix Pack 4 including installation-related instructions, prerequisites and corequisites, and list of fixes. All IBM Tivoli Key Lifecycle Manager for z/OS fix packs are cumulative.

Readme file for: IBM® Tivoli® Key Lifecycle Manager for z/OS
Product/Component Release: 1.0
Update Name: Fix Pack 4
Fix ID: 1.0.0-TIV-TKLM-FP0004
TKLM for z/OS Fix Pack 4 APAR: OA35100
Publication date: 24 January 2011
Last modified date: 24 January 2011

Contents

Platform support

Tivoli Key Lifecycle Manager platforms supported with initial release installed
z/OS V1 Release 9, or later

Download location

The distribution medium for the IBM Tivoli Key Lifecycle Manager Version 1.0 Fix Pack 4 PTF (FMID HCKL100, APAR OA35100) is magnetic tape or electronic download from ShopzSeries. The PTF contains the following SMP/E installable part:
CKLTB001 OA35100A HCKL100

Platforms updated by this fix pack.

Product/Component Name
IBM Tivoli Key Lifecycle Manager version 1.0 Fix Pack 4 - 1.0.0-TIV-TKLM-FP0004

Platform
z/OS V1 Release 9, or later

APAR
OA35100

Prerequisites and corequisites

None.

Known issues with TKLM for z/OS V 1.0 Fix Pack 4

- tklmDeviceAdd and tklmDeviceUpdate command line help do not reflect the DS8K changes to add partner certificates

    - The tklmDeviceAdd and tklmDeviceUpdate CLI commands incorrectly states that the value of aliasOne and aliasTwo for DS8K must be the same value. It also incorrectly states that if both aliases are specified with different values, aliasTwo value will be ignored and it will be set to the same value as aliasOne.

    - The tklmDeviceAdd and tklmDeviceUpdate CLI commands for DS8K now allow a partner certificate. Therefore, the value of aliasOne and aliasTwo for DS8K no longer have to be the same and they can be two different values. aliasOne is a required attribute and aliasTwo is optional.

- When user attempts to create the master keystore Tivoli Key Lifecycle Manager shows the following error:

  CTGKM0104E Unable to add keystore.javax.management.MBeanException: RuntimeException thrown in RequiredModelMBean while trying to invoke operation addKeyStore.

  The keystore path and file name must not be installed in the SSRE_APPSERVER_HOME\products\tklm\keystore\tklmKeystore.jceks. This filename is internally used by the Tivoli Key Lifecycle Manager keystore and the master keystore.

- When using Tivoli Key Lifecycle Manager command line interface (CLI) all parameters containing spaces must be enclosed in single quotes.

  For example:

  print AdminTask.tklmKeyStoreDelete ('-storeName "Tivoli Key Lifecycle Manager Keystore" -confirm y')

Known limitations with TKLM for z/OS V 1.0 Fix Pack 4

- Tivoli Key Lifecycle Manager for z/OS version 1.0 must be successfully SMP/E installed prior to the installation of the Tivoli Key Lifecycle Manager fix pack.

- Tivoli Key Lifecycle Manager version 1.0 backups taken using the "Backup and Restore" option in GUI or the tklmBackupRun CLI command without any fix pack installed cannot be restored once a fix pack has been applied.

- Problems can occur if you migrate keys that are members of multiple key groups in Encryption Key Manager to Tivoli Key Lifecycle Manager. The key is successfully migrated and made a member of the first key group. However, for subsequent key memberships, the migration code will log an error indicating the key and key group were not able to be migrated. You can use the migrated keys to read data, but cannot use the migrated keys to write from any group other than the first group membership that was successfully migrated. The error message is similar to this example:

  com.ibm.tklm.common.exception.KLMException: CTGKM0851E The group cannot be created because an entity (key) cannot be in multiple key groups.

  Contact support in order to complete migration. Do not install the fix pack until the migration is successful.

Installation information:

Installation instructions for the TKLM for z/OS V 1.0 Fix Pack 4 are located in README file, oa35100.pdf, at the following URL:

ftp://public.dhe.ibm.com/eserver/zseries/zos/tklm/pdf/oa35100.pdf

The TKLM for z/OS V 1.0 Fix Pack 4 README file references various sections of the TKLM V1.0 Infocenter, located at the following URL:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.tklm.doc/welcome.htm

Installing the Tivoli Key Lifecycle Manager fix pack.

Prior to fix pack installation

1. Ensure that Tivoli Key Lifecycle Manager is not being utilized before installing the fix pack. If your facility has a "service maintenance outage" process, consider installing this fix pack during an arranged service outage.

2. A backup of your Tivoli Key Lifecycle Manager server should be performed prior to installing this fix pack. Follow the steps 'Backing up critical files' in the Administering section of the Tivoli Key Lifecycle Manager product manuals.

Instructions

1. If this is a NEW install of TKLM for z/OS follow the instructions in the "IBM Tivoli Key Lifecycle Manager: Installation and Configuration Guide", chapter "Installing Tivoli Key Lifecycle Manager for z/OS", up to and including step 3, "SMP/E install Tivoli Key Lifecycle Manager for z/OS".

   If TKLM for z/OS has previously been installed skip all steps up to an including step 3.

   In either case, keep this section of the Installation and Configuration Guide open as we will follow it through the steps below.

2. Both NEW and PREVIOUS installs should SMP/E install the TKLM for z/OS Fix Pack 4 PTF (APAR OA35100).

3. Both NEW installs and PREVIOUS installs should follow step 4 to create a directory that will contain the fix pack packages and files. For example, create a directory containing the APAR name so it may easily be identified in the future.

   mkdir /tklmAparOA35100

   Note: For PREVIOUS installs DO NOT use the same directory that was used to install the original version of TKLM for z/OS V1 or any of the previous fix packs. The original install directory and all previous fix pack directories must be left intact as they will be needed by the fix pack install scripts to apply the fix pack.

   You must create a new directory for housing and installing the fix pack. It is recommended that a new filesystem be created for this new fix pack directory (mountpoint).

   For Sysplex installs, create a new unique directory on every subsystem that contains an instance of TKLM for z/OS. Each directory should be created under its associated subsystem root directory. For example:

   mkdir /SYSTEM_NAME/tklmAparOA35100

   The fix pack must be applied to each instance of TKLM for z/OS in order to bring all members of the Sysplex up to the fix pack level. Ensure that the following four steps, 4 through 7, are performed in parallel on each subsystem that contains an instance of TKLM for z/OS.

4. Both NEW installs and PREVIOUS installs should follow step 5 to give the SSRECFG and SSREGRP IDs ownership of the fix pack directory.

   chown SSRECFG:SSREGRP /tklmAparOA35100

5. Both NEW installs and PREVIOUS installs should follow step 6 to give the SSRECFG and SSREGRP IDs read, write, and execute permission of the fix pack directory.

   chmod 770 /tklmAparOA35100

6. Both NEW installs and PREVIOUS installs should follow step 7 to switch to the SSRECFG user ID.

su ssrecfg

7. Both NEW installs and PREVIOUS installs should follow step 8 to copy the fix pack tklm.tar file to the fix pack directory and extract its contents.

   cd /tklmAparOA35100
   cp /usr/lpp/tklm/tklm.tar /tklmAparOA35100/tklm.tar
   tar oxvfp tklm.tar

8. NEW installs should copy the 3 DB2 sample SPUFI scripts from the fix pack to a PDS.

   cp -T /tklmAparOA35100/samples/tklmsql_zos_install.db2
   "//'TKLM.SPUFI.OA35100(tklmdb2i)'"
   cp -T /tklmAparOA35100/samples/tklmsql_zos_uninstall.db2
   "//'TKLM.SPUFI.OA35100(tklmdb2u)'"
   cp -T /tklmAparOA35100/samples/tklmsql_zos_migrate.db2
   "//'TKLM.SPUFI.OA35100(tklmdb2m)'"

   Note: PREVIOUS installs should already have a customized version of the sample SPUFI scripts from when Fix Pack 1 was applied and can skip this step.

   For New Sysplex installs, if you are running DB2 in datasharing mode between all subsystems within your parallel sysplex, you should only copy the fix pack sample SPUFI scripts to one subsystem's PDS.

9. NEW installs should follow Step 10, 11, and 12 for DB2 setup, SMF setup, and migration preparation. New installs should not run the sample SPUFI migrate script, tklmsql_zos_migrate.db2.

   PREVIOUS installs should already have an updated TKLM Database in place as a result of applying Fix Pack 1 and can skip this step.

   Note: For NEW Sysplex installs, if you are running DB2 in datasharing mode between all subsystems within your parallel sysplex, you should only customize and execute the sample SPUFI script on one subsystem.

   For NEW installs, the sample SPUFI scripts, tklmsql_zos_install.db2, will create a new TKLM Database with name TKLMDBFP.

10. NEW installs and PREVIOUS installs that need to create or change their installation parameters (for example the SSRECFG password) should follow step 13 to create a new TKLM response file.

    PREVIOUS installs who have a valid TKLM response file may continue to use it to install the fix pack and skip this step.

    /tklmAparOA35100/bin/createResponseFile.sh

    Note: For Sysplex installs, if you need to create or change your installation parameters you will need to perform this step on all subsystems.

11. NEW Installs should follow step 14 to install a new copy of TKLM at this fix pack level.

PREVIOUS installs should instead run the updateTKLM.sh script located within the fix pack.

The -previousVersion flag is a mandatory argument of the updateTKLM.sh script that is used to point to your previous install directory of TKLM for z/OS.

For Fix Pack 4 the previous install directory should be a prior install directory, for example the Fix Pack 3 install directory.

New Installs:
/tklmAparOA35100/bin/installTKLM.sh

Previous Installs:
/tklmAparOA35100/bin/updateTKLM.sh -previousVersion /tklmAparOA30120

Note: Sysplex installs will need to perform this step on all subsystems.

12. Optionally both NEW and PREVIOUS installs may follow step 15 to configure file based auditing.

13. NEW installs should follow steps 16, 17, and 18 for RACF Keyring setup and to configure SSRE to use available authentication data when an unprotected URI is accessed.

    PREVIOUS installs should skip this step.

    Note: NEW Sysplex installs will need to perform this step on all subsystems.

Performing the necessary tasks after fix pack installation.

1. Both NEW installs and PREVIOUS installs should verify the fix pack installation by following step 19 and ensuring that TKLM is listed on the ISC Console welcome page at Version 1.0.0.4.

2. A backup of your Tivoli Key Lifecycle Manager server should be performed after installing this fix pack. Follow the steps 'Backing up critical files' in the Administering section of the Tivoli Key Lifecycle Manager Product Manuals.

   Note: For additional information on installing TKLM for z/OS within a Parallel Sysplex read the next section of the Tivoli Key Lifecycle Manager Product Manuals, "Installing Tivoli Key Lifecycle Manager on z/OS Parallel Sysplex systems".

Recovering from a failed fix pack installation

Steps for rolling back Tivoli Key Lifecycle Manager for z/OS Version 1, z/OS V1 Release 9, or later.

Instructions

1. Start an OMVS session and switch to the SSRECFG user ID.

   su ssrecfg

2. Change directory to the location of the fix pack install directory.

   cd /tklpmAparOA35100

3. Run the updateTKLM.sh script with the -recover and -previousVersion flags.

   The -previousVersion flag is a mandatory argument of the updateTKLM.sh script that is used to point to your previous install directory of TKLM for z/OS.

   For Fix Pack 4 the previous install directory should be a prior install directory, for example the Fix Pack 3 install directory.

   /tklmAparOA35100/bin/updateTKLM.sh -recover -previousVersion /tklmAparOA30120

   Note: For Sysplex installs, steps 1, 2 & 3 above must be performed on all subsystems that contain an instance of TKLM at the Fix Pack 4 level in order to roll back to a prior level.

Fix pack installation error conditions

Exit Code - Description - Possible Causes, Recovery Actions

2 - Uninstall Failed - The uninstall script failed to uninstall all TKLM components. See the log file in /tklmAparOA35100/logs for more information.

3 - TKLM Fix Pack Install Failed - The install script failed to install all TKLM components. See the log file in /tklmAparOA35100/logs for more information.

4 - TKLM Database Connection Failure - TKLM's failed to connect to DB2. Ensure that your DB2 user ID has access to the TKLM database and your password is correct.

5 - Cannot Create Log File - The TKLM scripts were unable to create a log file in the /tklmAparOA35100/logs directory. Ensure that the /tklmAparOA35100/logs directory is owned by the SSRECFG user ID and SSREGRP group ID, and that the permissions are set to 770 (read, write, and execute for owner and group). Also ensure that you are logged on as the SSRECFG user ID.

8 - Cannot Backup Config Files - The TKLM update script failed to backup the TKLM configuration files. Ensure that the /tklmAparOA35100 directory is owned by the SSRECFG user ID and SSREGRP group ID, and that the permissions are set to 770 (read, write, and execute for owner and group). Ensure that the TKLM_HOME directory within the SSRE config HFS allows the SSRECFG user ID read and write access. Also ensure that you are logged on as the SSRECFG user ID.

9 - Cannot Restore Config Files - The TKLM update script failed to restore the TKLM configuration files. Ensure that the /tklmAparOA35100 directory is owned by the SSRECFG user ID and SSREGRP group ID, and that the permissions are set to 770 (read, write, and execute for owner and group). Ensure that the TKLM_HOME directory within the SSRE config HFS allows the SSRECFG user ID read and write access. Also ensure that you are logged on as the SSRECFG user ID.

10 - Log Directory is a File - The TKLM scripts failed to create a log file within the /tklmAparOA35100/logs directory because /tklmAparOA35100/logs is a file, not an actual directory. Rename the /tklmAparOA35100/logs file to something else, and create a new directory named /tklmAparOA35100/logs. This directory should be owned by the SSRECFG user ID and SSREGRP group ID, and the permissions should be set to 770 (read, write, and execute for owner and group).

11 - Database Migration Failed - There was a failure with the database migration. See the log file for more information.

12 - Invalid TKLM Version - Either the fix pack level you are trying to install or the previous level you are pointing to with the -previousVersion flag is not valid. Execute the /tklmAparOA35100/bin/versionInfo.sh script to ensure you are installing z/OS Service Level: OA35100, and execute the /tklmProductInstall/bin/versionInfo.sh to ensure your previous version is a valid TKLM for z/OS fix-pack id.

15 - Log Directory Does Not Exist - The TKLM scripts failed to create a log file because the /tklmAparOA35100/logs directory does not exist. Create a new directory named /tklmAparOA35100/logs. This directory should be owned by the SSRECFG user ID and SSREGRP group ID, and the permissions should be set to 770 (read, write, and execute for owner and group).

20 - No Response File Found - The TKLM scripts failed to find a response file. Use the -responseFile flag to specify a valid response file, or create a new response file using the /tklmAparOA35100/bin/createResponseFile.sh script.

25 - Cannot Create Response File - The createResponseFile.sh script failed to create a response file. Ensure that the directory where you are trying to create the response file is owned by the SSRECFG user ID and SSREGRP group ID, and the permissions are set to 770 (read, write, and execute for owner and group). If no path is specified the default response file will be written to /tklmAparOA35100/bin/tklmInstall.response

30 - Cannot Update Response File - The createResponseFile.sh script failed to create a response file. Ensure that the directory where you are trying to create the response file is owned by the SSRECFG user ID and SSREGRP group ID, and the permissions are set to 770 (read, write, and execute for owner and group). If no path is specified the default response file will be written to /tklmAparOA35100/bin/tklmInstall.response

35 - Invalid Input - Invalid input was passed to the TKLM script. Run the script again with valid input.

40 - Invalid Response File - The response file passed to the TKLM script is not valid. Create a new response file using the /tklmAparOA35100/bin/createResponseFile.sh script.

45 - Cannot Create SSRE Product Directory - There was a failure when creating the SSRE product directory. This directory is located within your SSRE config HFS under SSRE_APPSERVER_HOME. Ensure that the SSREGRP group has read, write, and execute permission of the SSRE_APPSERVER_HOME directory.

50 - Cannot Create TKLM Product Directory - There was a failure when creating the TKLM product directory. This directory is located within your SSRE config HFS under SSRE_APPSERVER_HOME/products. Ensure that the SSREGRP group has read, write, and execute permission of the SSRE_APPSERVER_HOME/products directory.

55 - TKLM UI/Server Install Failed - There was a failure when deploying the TKLM binaries within SSRE. Ensure that the SSRE Config HFS is not full and that the SSREGRP group has read, write, and execute permission of the SSRE_APPSERVER_HOME directory. Also ensure that the contents of the /tklmAparOA35100/bin directory are owned by the SSRECFG user ID and SSREGRP group ID, and the permissions are set to 770 (read, write, and execute for owner and group).

60 - Cannot Start WAS Server - There was a problem starting SSRE. Ensure that you have specified the correct password for the SSRECFG user ID within the response file or by using the -wasPassword flag. Try stopping SSRE from the console and running the TKLM script again.

65 - Cannot Stop WAS Server - There was a problem stopping SSRE. Ensure that the TKLM key server is not busy serving keys and attempt to stop SSRE from the console. If SSRE will not stop from the console you may need to cancel it before you can run the TKLM script again.

70 - Database Configuration Failure - There was a problem configuring the database connection. Ensure that you have specified the correct DB2 parameters in the response file and that DB2 is started on the system.

75 - Copy Failure - A file copy failed. Ensure that the file system is not full and that the SSRECFG ID has write permission to copy the file to the destination.

80 - Plugin Initialization Failure - The TKLM binaries failed to initialize within SSRE. Ensure that the SSRE Config HFS is not full and that the SSREGRP group has read, write, and execute permission of the SSRE_APPSERVER_HOME directory. Also ensure that the contents of the /tklmAparOA35100/bin directory are owned by the SSRECFG user ID and SSREGRP group ID, and the permissions are set to 770 (read, write, and execute for owner and group).

85 - Invalid Response File - The response file passed to the TKLM script is not valid. Create a new response file using the /tklmAparOA35100/bin/createResponseFile.sh script.

90 - Error In Migration - The EKM to TKLM migration failed. Ensure that the EKM files and configuration is valid.

95 - TKLM Already Installed - A TKLM install failed because TKLM is either installed or in a partially installed state. Use the update script, /tklmAparOA35100/bin/updateTKLM.sh, to update TKLM to the fix pack, or use the uninstall script, /tklmAparOA35100/bin/uninstallTKLM.sh, to uninstall TKLM.

99 - Internal Error - There was an internal error while running the TKLM scripts. See the log file in the /tklmAparOA35100/logs directory for more information.

List of fixes

APAR fixes included in TKLM for z/OS v 1.0 Fix Pack 4

APAR No. - Sev. - Abstract

OA35210 - 3 - TKLM for z/OS DID NOT FAIL OVER AFTER LOSS OF KEYSTORE PROVIDER

IZ81352 - 3 - THE REFERENCE GUIDE FOR TKLM v1 IMPLIES THAT THE COMMAND TKLMGROUPENTRYADD WILL ACCEPT MULTIPLE KEY VALUES OR ALIAS RANGE (Documenation Change)

IZ84588 - 3 - IMPROVEMENTS IN CRYPTOGRAPHIC OPERATION HANDLING FOR FIPS 140-2 MODE

IZ84600 - 3 - KEY EXPORT FAILURE WHEN FIPS IS ENABLED

IZ84617 - 2 - KEYSERVER ERROR HANDLING WHEN DB2 IS NOT RESPONDING OR DOWN

IZ84618 -3 - JAG4 ENABLEMENT

Copyright and trademark information
http://www.ibm.com/legal/copytrade.shtml
Notices
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.
This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.
Microsoft, Windows, and Windows Server are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
Other company, product, or service names may be trademarks or service marks of others.
THIRD-PARTY LICENSE TERMS AND CONDITIONS, NOTICES AND INFORMATION
The license agreement for this product refers you to this file for details concerning terms and conditions applicable to third party software code included in this product, and for certain notices and other information IBM must provide to you under its license to certain software code. The relevant terms and conditions, notices and other information are provided or referenced below. Please note that any non-English version of the licenses below is unofficial and is provided to you for your convenience only. The English version of the licenses below, provided as part of the English version of this file, is the official version.
Notwithstanding the terms and conditions of any other agreement you may have with IBM or any of its related or affiliated entities (collectively "IBM"), the third party software code identified below are "Excluded Components" and are subject to the following terms and conditions:
* the Excluded Components are provided on an "AS IS" basis
* IBM DISCLAIMS ANY AND ALL EXPRESS AND IMPLIED WARRANTIES AND CONDITIONS WITH RESPECT TO THE

EXCLUDED COMPONENTS, INCLUDING, BUT NOT LIMITED TO, THE WARRANTY OF NON-INFRINGEMENT OR INTERFERENCE AND THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

* IBM will not be liable to you or indemnify you for any claims related to the Excluded Components
* IBM will not be liable for any direct, indirect, incidental, special, exemplary, punitive or consequential damages with respect to the Excluded Components.

End of Document