Release Notes

IBM® Tivoli® Identity Manager

RACF Adapter

Version 4.6.10

Fourteenth Edition (April 21, 2010)

This edition applies to version 4.6 of this Adapter and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Preface

Welcome to the IBM Tivoli Identity Manager RACF Adapter.

These Release Notes contain information for the following products that was not available when the IBM Tivoli Identity Manager manuals were printed:

- IBM Tivoli Identity Manager RACF Adapter Installation and Configuration Guide

Adapter Features and Purpose

The RACF Adapter is designed to create and manage RACF accounts. Typically, one adapter is installed per RACF Database, but the RACF Adapter may be configured to support a subset of the accounts through the Scope-of-Authority Feature on the RACF Service Form. The optimum deployment configuration is based, in part, on the configuration of your zOS systems, but the primary factor is the planned structure of your Identity Manager Provisioning Policies and Approval Workflow process. Please refer to the Identity Manager Policy, Organization & Administration Guide for a discussion of these topics.

The RACF Adapter is a powerful tool that requires Administrator Level authority. The Adapter operates much like a human system administrator, creating accounts, connecting to groups, and assigning other privileges. Operations requested from the Identity Manager server will fail if the Adapter is not given sufficient authority to perform the requested task. IBM recommends that this Adapter run with administrative permissions.

Special note 1: This release of the ITIM RACF adapter will work with ITIM 4.6, or ITIM 5.0.

Special note 2: The RACF adapter profile, to be installed on the ITIM server, has changed. All Boolean attributes are now directory strings. This prevents ITIM from sending to the RACF adapter Boolean attributes that have not been set or reset. Additionally, the RACF account form has changed these attributes to reflect a drop-down selection, allowing specification of TRUE, FALSE, or “unspecified”.

Contents of this Release

Adapter Version

Component	Version
Release Date	April 21, 2010
Adapter Version	4.6.10 (build 4.6.1013)
Common Libraries	ADK v4.81zOS
Documentation	ITIM RACF Adapter Installation and Configuration Guide v4.6.0 SC32-1490-08

New Features

Enhancement # (FITS)	Description
	Items included in current release
OSDB	Added support for RACF 1.11.
	Items included in 4.6.9 release
MR0420095719	RACF adapter tested for compatibility with z/OS 1.10. The adapter is compatible with version 1.10 but does not support new 1.10 features such as schema extension and passphrase.
	Items included in 4.6.8 release
MR1127071942	Two-way SSL (Client authentication) is now supported.
N/A	This release of the ITIM RACF adapter has been updated so that it is compatible with TIM 5.0 and will upgrade easily. The RACF adapter profile, to be installed on the ITIM server, has changed. All Boolean attributes are now directory strings. This prevents ITIM from sending to the RACF adapter Boolean attributes that have not been set or reset. Additionally, the RACF account form has changed these attributes to reflect a drop-down selection, allowing specification of TRUE, FALSE, or "unspecified". NOTE: the TIM UI has changed. Please review the impact of this change on your Provisioning Policies or third-party integrations.
MR0212086159	Documentation update: Include extra columns in the attribute tables, so the commands to add or delete an attribute would be documented. NOTE: the TIM v5.0 Installation and Configuration Guide contains this additional information and has been included in this distribution.

Enhancement # (FITS)	Description
MR0516075819 MR0816061418	Allow the ITIM server to optionally pass the “erRacuPwNoexpire” attribute to this adapter. This attribute MUST accompany the password, on a password change request. A sample of how this is accomplished through an ITIM workflow is provided as a whitepaper.
	Items included in prior releases
MR0302052537 (APAR IY68535)	Implemented a new agent option “SHORTCONNECT”. This option has two values; “TRUE” and “FALSE”. If this agent option is not specified, it defaults to “FALSE”. Those who wish to use this capability, please reference the section “Corrections to install guide” below.
MR0326075124	z/OS DBCS data is not properly interpreted by the agent. z/OS DBCS data is now properly translated and escaped, where necessary. This backs out (supersedes) APAR IY78356, as unprintable data is now properly replaced by “?” (question marks).

Closed Issues

DevTrack	APAR#	PMR# / Description
		Items included in current release
		None
		Items included in 4.6.9 releases
	IZ19603	63772,999,000 Erracupwnoexpire attribute passed in with a password change request is not being honored correctly. In all cases, the result was a non-expired password.
		Items included in 4.6.8 releases
	IZ18723	39839,211,788 Abend S0CF (floating point divide exception) occurs, when the adapter is configured for event notification, at the end of a reconciliation or an event notification interval.
		Items included in prior releases
	IY97572	40029,379,000 Prior to the change, the adapter would hang (with CLOSE_WAIT TCP connections), and MAXTHREADS having been reached and transactions directed to the RACF adapter would remain in pending state in the ITIM server. We've identified an API we are now using, which allows the threads to properly clean up upon termination. Before the use of this API, although the threads were in fact going away, apparently, the Unix System Services thread count was NOT being decremented. Now, with the use of this API call, the MAXTHREADS problem is alleviated.
	IY96074	07139,080,678 RACF adapter incurs an ABEND0C4 (or S328) at startup, due storage not being initialized in console interface.
	internal	N/A In the agent schema, erracuopauth attribute was marked as single valued. It is now correctly marked as multi-valued.
S17549	IY89301	78771,499,000 Adapter goes into a loop, when the TCPIP communications stack is stopped. Code was changed to abnormally terminate the adapter, when TCPIP is stopped.

DevTrack	APAR#	PMR# / Description
S17250	IY82747	23708,379,000 ABEND0C4 when Language Environment default options set "TRAP(OFF)".
S17430	IY85993	58033,379,000 Agent consumes excessive storage during reconciliation. By default the agent buffers 3000 entries to be sent to server, before putting the agent into a wait. This may now be externally controlled through an added environment variable "PDU_ENTRY_LIMIT". The generated startup script for the agent will now have this environment variable specified, with a value of 500. This may be adjusted at the customer site to a different value. For existing installations, you may specify this value in the existing startup script (by default, **racfagent.sh**)
S17058	IY78356 (now superceded)	N/A There are situations where invalid characters appear in RACF data. This data is unusable by RACF, but causes the ITIM server to abnormally terminate the reconciliation. With this APAR, unprintable data is returned to the ITIM server as question marks "?". This data typically is found in RACF data fields populated by the user, such as the TSO logon command string, however, all character data will pass through this validation.
S17161	IY79827	70193,227,000 Storage leak occurs, when the communications connection is broken between the ITIM server and the adapter, during a reconciliation. Entries were being orphaned, once the connection was lost. Entries are now deleted, and the reconciliation is terminated, if the connection is lost.
S72169	IY72169	36578,001,806 On IPV4-only versions of OS/390 and z/OS (1.3 and prior, ABEND0C4 results when connection from ITIM server is attempted.
S16041	-none-	N/A Case sensitivity issue on RACFacct in Customlabels.properties file in the profile .jar file.
S16135	IY68782	29553,122,000 When PASSEXPIRE is defaulted to TRUE, or set to TRUE or TRUEADD, the password is not being set.

Known Issues

DevTrack	APAR#	PMR# / Description
		None.

Installation and Configuration Notes

See the IBM Tivoli Identity Manager RACF Adapter Installation Guide for detailed instructions.

Corrections to Installation Guide

The following corrections to the Installation Guide apply to this release:

For enhancement MR0302052537, the Tivoli Identity Manager 4.6 RACF Adapter Installation and Configuration Guide, form number SC32-1490-08, Appendix B, Table 23, has the following addition:

Option Attribute	Default Value	Valid values	Function and meaning	Required?
SHORTCONNECT	FALSE	TRUE, FALSE	When defaulted, or set to FALSE, full RACF connect entries are returned to the ITIM server. When this option is set to TRUE, RACF connect entries returned to the ITIM server will have 5 fewer attributes returned in the erRacConXML values.	No

The standard behavior of the reconciliation function in the RACF adapter is to return all data back to the ITIM server. This option alters that behavior. The use of this option, this may lessen, or eliminate, the need for use of the “custom policy join directive”.

This option addresses an ITIM policy implementation issue, when building a provisioning policy for RACF accounts. When a straight string compare is performed between the “policy” version of a connect entry, and the value in the erRacConXML, the policy will always return a mismatch between the two. This is because of the transient behavior of creation date, last logon date/time, logon count, and future revoke/resume dates. With this option enabled, these dynamic attributes will be omitted. The revoke and resume dates are also omitted, as this prevents a RACF user from being RESUMEd, because of the difference between the connect entry and the policy.

The following figure indicates the content of a single value, within the erRacConXML attribute. The items that are ***bolded*** and ***italicized*** are omitted when the SHORTCONNECT option is set to TRUE:

```
<CONNECT_ENTRY name="CONENTRY">
<ADSP>FALSE</ADSP>
<AUDITOR>FALSE</AUDITOR>
<AUTHORITY>USE</AUTHORITY>
<DATE>2003121012002</DATE>
<GRPACC>FALSE</GRPACC>
<LAST_DATE>2003121012002</LAST_DATE>
<LOGON_COUNT>0</LOGON_COUNT>
<OPERATIONS>FALSE</OPERATIONS>
<OWNER>CONENTRY</OWNER>
<RESUME_DATE>2003121012002</RESUME_DATE>
<REVOKE_DATE>2003121012002</REVOKE_DATE>
<REVOKED>FALSE</REVOKED>
<SPECIAL>FALSE</SPECIAL>
<UACC>NONE</UACC>
</CONNECT_ENTRY>
```

Configuration Notes

The following additions to the Installation Guide apply to this release:

1. If you are just upgrading an already installed Adapter with version 4.5.6 (build 1018) or earlier, you must completely re-install and configure the adapter. NOTE: The RACF SSL agent is NOT an upgrade of the RACF FTP agent. While many of the features are the same, the schema and all attributes and Object Classes are different. Moving from RACF FTP to RACF SSL is a MIGRATION not an upgrade. A Schema Migration Tool is available to assist with this migration. Please contact ITIM Level 2 support for more information.

2. Once the "config.sh" script has been executed in the Unix System Services environment, the adapter registry file MUST be "CHOWN"ed to give ownership of this file to the RACF ID that the RACF adapter runs under. Failure to do this will prevent the adapter from initializing.

   In lieu of doing this as SUPERUSER, the installation may wish to delegate this authority to the owning user, by defining in the RACF UNIXPRIV class a profile of CHOWN.UNRESTRICTED. This allows the owner of a file the ability to issue a USS "chown" command, giving ownership of the file to another user and group. Example: "**`chown –R itiagnt:agentgrp /u/itim`**"

   Another method of accomplishing this is to allow the configuration of the adapter be accomplished by signing on as the same RACF ID the adapter will run under. This will require the adapter RACF ID to have temporary access to TSO, and the OMVS shell to accomplish this.

   Yet another method would be to have the installing RACF user ID to share the same OMVS UID as the ID of the adapter that will execute.

   Bottom line is, it is required the ownership of the directory structure be the ID of the agent user ID. This can be accomplished by:
   a. SUPERUSER (UID 0) performing the "chown" command, following installation by a different UID, to change ownership to the adapter's RACF user ID.
   b. If superuser is not available, the installation have the RACF class UNIXPRIV CHOWN.UNRESTRICTED profile defined allowing the installing RACF user ID, following installation, to issue the "chown" command.
   c. Or the installation be performed using the RACF user ID of the adapter itself.

3. It is suggested, although not necessary, to set the SYSTSPRT DD statement, in the ITIMCMD transaction JCL to "DUMMY". For normal processing, when debugging is not necessary, it will prevent sysout files from being produced during the normal course of operation. During normal processing, without debugging, only two lines are generated. When debugging is necessary, however, it will be required to reflect SYSOUT= so that debugging information can be recorded.

4. The default number of threads for the RACF adapter is 100. This is a recommended setting, and should not require adjustment.

5. It is recommended that you have defined _BPX_SHAREAS=YES in /etc/profile. This allows the Adapter to run in a single address space, instead of multiple address spaces. By running with this environment variable, it gives the desired effect that the started task may be stopped using the same name it was started with. Since this has effect throughout Unix System Services, it would be prudent to check the USS documentation. Refer to z/OS UNIX System Services Planning, document GA22-7800 for more details.

6. Insure the TZ environment variable in /etc/profile is defined correctly for your timezone. This will allow messages in the Adapter log to reflect proper local time. Refer to z/OS UNIX System Services Planning, document GA22-7800 for more details.

7. In the documentation, it is recommended the agent run with RACF SPECIAL and AUDITOR. The AUDITOR attribute is NOT required, nor necessary for proper operation, however, warnings may occur in transactions, where the setting or unsetting of the UAUDIT attribute is attempted. This may be addressed by removing the UAUDIT attribute from the RACF form on the ITIM server user interface customization.

Supported Configurations

Installation Platform

The IBM Tivoli Identity Manager Adapter was built and tested on the following product versions.

Adapter Installation Platform:
z/OS 1.4, 1.5,1.6,1.7,1.8, 1.9, 1.10 and 1.11

Managed Resource:
IBM Security Server (RACF) on zOS

IBM Tivoli Identity Manager:
ITIM 4.6.0

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

```
IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY  10504-1785
U.S.A.
```

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

```
IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan
```

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: 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 states 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.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged should contact:

```
IBM Corporation
2ZA4/101
11400 Burnet Road
Austin, TX 78758  U.S.A.
```

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
DB2
IBM
IBM logo
SecureWay
Tivoli
Tivoli logo
Universal Database
WebSphere

Lotus is a registered trademark of Lotus Development Corporation and/or IBM Corporation.
Domino is a trademark of International Business Machines Corporation and Lotus Development Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

End of Release Notes