Release Notes

IBM® Tivoli® Identity Manager

RACF Adapter

Version 5.0.11

Second Edition (February 28, 2012)

This edition applies to version 5.0 of Tivoli Identity Manager 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. The adapter runs in ”agent” mode and must be installed on z/OS. 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 deployment configuration is based, in part, on the topology of your network domain, but the primary factor is the planned structure of your Identity Manager Provisioning Policies and Approval Workflow process. Please refer to the Identity Manager Information Center for a discussion of these topics.

The Identity Manager Adapters are powerful tools that require administrator level authority. Adapters operate much like a human system administrator, creating accounts, permissions and home directories. 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 (root) 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	February 28, 2012
Adapter Version	5.0.11
Component Versions	Adapter Build 5.1.1021 Profile 5.0.1002 ADK 5.22 z/OS
Documentation	RACF Adapter Installation and Configuration Guide SC23-6162-02 NOTE: this version of the adapter was designed for TIM 5.1 but it is being made available to TIM 5.0 customers as well. The Installation Guide refers to TIM 5.1, but applies also to TIM 5.0.

New Features

Enhancement # (FITS)	Description
	Items included in current release
OSDB Update	RACF Adapter and z/OS V1R13 support
	Items included in 5.0.10 release
MR1108102228	RACF Adapter and z/OS V1R12 support
	Items included in 5.0.7 release
MR1026063837 MR0523074234	Enhanced the adapter to call the ITIMEXIT program on account modify request.
N/A	Updated installation procedure to use ISPF
	Items included in 5.0.6 release
	Add support for RACF on z/OS V1R11
	Items included in 5.0.5 release
	None
	Items included in 5.0.4 release
MR0420095719	RACF adapter tested for compatibility with z/OS V1R10. 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 5.0.3 release
MR1127071942	Two-way SSL (Client authentication) is now supported.
N/A	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.

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 “Configuration Notes” 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

Internal#	APAR#	PMR# / Description
		Items included in current release
N/A	IV01401	Three RACF OPERPARM segment attributes are incorrect: ERRACUOPAUTH incorrectly returns “MSTR” instead of “MASTER” on a reconciliation. ERRACUOPLEVEL requires a value of "I". ERRACUOPMFORM requires a value of "J". ERRACUOPMFORM and ERRACUOPMONITOR incorrectly returned on a reconciliation.
N/A	IV14398	RACF adapter to include a timeout setting.
		Items included in 5.0.10
N/A		N/A SearchRequest attributes not set correctly so reconciliation under a requester ID not honoured correctly.
	N/A	13681,112,848 certTool generating corrupt CSRs
	IZ86303	RACF and ACF2 adapter with 2-way SSL (Register certificate). Registered certificates giving 'Subject validation failed' message even when correctly registered.
	IZ92541	Minor corrections to the new RACF adapter installation dialog.
	IZ94090	RACF adapter failure during reconciliation - FIX0205: FAILED, RC= 16. Correction to reconciliation transaction JCL.
	IZ94640	The data sets are not allocated correctly in an non-sms environment
	IZ94656	RACF adapter reconciliation does not return select 'boolean' values.
	IZ95315	RACF adapter post modify option is in the wrong place
	IZ95829	RACF adapter 5.1.3 missing registry settings in the documentation.
	IZ96327	Response message for request shows a parsing error. Error: An invalid XML character (Unicode: 0x1a) was found in the value of attribute "matchedDN" and element is "LDAPResult”
	IZ98511	Error modifying connected groups.
		Items included in 5.0.7
N/A		N/A Corrections to future revoke date and future resume date processing. They must be processed in date order if both are specified on the same add or modify request. Also the dates are now reset correctly, if no date is specified, and a resume or revoke date already exists.
N/A		N/A

		The maximum length of 20 for the attribute RACF UserName (erracuname) must be enforced in the profile.
		Items included in 5.0.6 release
		None

Internal#	APAR#	PMR# / Description
		Items included in 5.0.5 release
	N/A	N/A Removed obsolete xforms from the profile.jar.
		Items included in 5.0.4 releases
	IZ52887	63572,370,000 RACF Certificate installation documentation is incorrect. See “Configuration Section” of this document for more information.
		Items included in 5.0.3 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 5.0.2 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 5.0.1 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.

Internal#	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 2000. 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.

Known Issues

Internal#	APAR#	PMR# / Description
	N/A	This release of the RACF Adapter does not support FIPS.

Installation and Configuration Notes

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

Upgrading to Version 5.0.11 (or later)

If you are upgrading an adapter with ADK 4.81 z/OS 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.

Instructions for upgrading version 5.1 (upgrading from version 4.6 or earlier will require a full install): Refer to the Installing and configuring section of the RACF adapter guide for full details.

1) Upload the XMI file and install the ISPF dialog as described in the “Installing and configuring the adapter” chapter of the RACF adapter guide.
2) Run the ISPF dialog and load previously saved variables using option 1, then generate the job streams using option 3. This generates the JCL in userid.ITIMRACF.CNTL and populates userid.ITIMRACF.DATA.
3) Assuming installing directly over an existing, working adapter running on ADK version 5.17+ with no changes to the installation parameters (the saved variables), then the only installation jobs in data set userid.ITIMRACF.CNTL that need to be submitted:

J3: This job allocates and populates the load and exec data sets, and populates the OMVS directories. You may require superuser authority to submit this job successfully.
J6: This job registers the APPC/MVS transactions.

This release contains a new profile, so this must be imported into the Tivoli Identity Manager server as described in the "Configuring communication" section of the RACF adapter guide.

Corrections to Installation Guide

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

Unix System Services (USS) Adapter read-only home and read/write home

The read-only home and the read/write home must specify different locations. If they are the same then the installation may fail.

Scoped reconciliation VSAM data set

If no scoped reconciliation VSAM data set is defined during the installation process, then the attribute SCOPING=FALSE will be set in the registry. If scoped reconciliation is required in the future then the installation panels must be used again to generate J6 and J8, and these jobs submitted. Then the attribute SCOPING=TRUE must be set using agentCfg tool.

Starting and stopping the adapter

Before you start the adapter, ensure that TCP/IP is active, and the APPC/MVS and the ASCH address spaces are active.

Modifying protocol configuration

Table 7. Options for the DAML protocol menu

Option	Configuration task
K	Displays the following prompt: Modify Property 'READ_TIMEOUT': Specify the timeout value in seconds. The default is 0 and means that no read timeout is set. Note: READ_TIMEOUT is provided to prevent threads being left open in the adapter and causing 'hang' problems. The open threads may be due to firewalls, or network connections problems, and may be seen as TCP/IP ClosWait connections remaining on the adapter. If you encounter such problems, then you need to set the value of READ_TIMEOUT to just longer than the ITIM manager timeout (the maximum connection age DAML property on Tivoli Identity Manager) and less than any firewall timeout. The adapter will then need to be restarted as READ_TIMEOUT is set at adapter initialization.

Configuration Notes

The following configuration notes apply to this release:

Short Connect Group Feature

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>200312101200Z</DATE>
<GRPACC>FALSE</GRPACC>
<LAST_DATE>200312101200Z</LAST_DATE>
<LOGON_COUNT>0</LOGON_COUNT>
<OPERATIONS>FALSE</OPERATIONS>
<OWNER>CONENTRY</OWNER>
<RESUME_DATE>200312101200Z</RESUME_DATE>
<REVOKE_DATE>200312101200Z</REVOKE_DATE>
<REVOKED>FALSE</REVOKED>
<SPECIAL>FALSE</SPECIAL>
<UACC>NONE</UACC>
</CONNECT_ENTRY>
```

Customizing or Extending Adapter Features

The Identity Manager adapters can be customized and/or extended. The type and method of this customization may vary from adapter to adapter.

Getting Started

Customizing and extending adapters requires a number of additional skills. The developer must be familiar with the following concepts and skills prior to beginning the modifications:

- LDAP schema management
- Working knowledge of scripting language appropriate for the installation platform
- Working knowledge of LDAP object classes and attributes
- Working knowledge of XML document structure

Note: This adapter supports customization only through the use of pre-Exec and post-Exec scripting. The RACF adapter also has REXX scripting options. Please see the RACF Installation and Configuration guide for additional details.

Tivoli Identity Manager Resources:

> Check the “Learn” section of the Tivoli Identity Manager Support web site for links to training, publications, and demos.

Support for Customized Adapters

The integration to the Identity Manager server – the adapter framework – is supported. However, IBM does not support the customizations, scripts, or other modifications. If you experience a problem with a customized adapter, IBM Support may require the problem to be demonstrated on the GA version of the adapter before a PMR is opened.

Supported Configurations

Installation Platform

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

Adapter Installation Platform:
RACF on z/OS V1R11, V1R12 and V1R13

Managed Resource:
IBM Security Server (RACF) for z/OS

IBM Tivoli Identity Manager:
Identity Manager v5.0

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:

IBM
IBM logo
Tivoli
RACF

Adobe, Acrobat, Portable Document Format (PDF), and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. 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.

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.

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

Linux is a trademark of Linus Torvalds in the U.S., other countries, or both.

End of Release Notes