Release Notes

IBM

IBM® Security Identity

CA ACF2 for z/OS Adapter

First Edition (June 14, 2019)

This edition applies to the latest version of IBM Security Identity Adapter for ACF2 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Table of Contents

Preface

Welcome to the IBM Security Identity Adapter for CA ACF2.

These Release Notes contain information for the following products that was not available when the IBM Security Identity server manuals were created:

- IBM Security Identity Manager CA ACF2 for z/OS Adapter Installation and Configuration Guide
- IBM Security Privileged Identity Manager CA ACF2 for z/OS Adapter Installation and Configuration Guide
- IBM Security Identity Governance and Intelligence CA ACF2 for z/OS Adapter Installation and Configuration Guide

Adapter Features and Purpose

The CA ACF2 for z/OS Adapter is designed to create and manage CA ACF2 for z/OS accounts. The adapter runs in "agent" mode and must be installed on z/OS. One adapter is installed per CA ACF2 installation..

The IBM Security Identity 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 IBM Security Identity 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.

License Agreement

Review and agree to the terms of the IBM Security Identity product license prior to using this product. The license can be viewed from the "license" folder included in the product package.

Contents of this Release

Adapter Version

Component	Version
Build Date	June 13, 2019
Adapter Version	7.1.29
Component Versions	Adapter Build 7.1.0029.00 Profile 7.1.0029 ADK 6.06.0012 z/OS enRole Resource Management API 6.0.6 OpenSSL 1.0.2q
Documentation	Please find the latest documentation using the IBM Security Identity Manager Knowledge Center. Select the latest server release to navigate to the latest version of the adapter documentation.

New Features

Internal#	RFE/CASE#	Description
		Items included in current release
		No changes in the current release
		Items included in 7.1.28 release
		No changes in the current release
		Items included in 7.1.27 release
RTC 182213		IGI 5.2.5 support - As an adapter developer for z/OS I need to add support for supporting data and canonical values to the IGI profiles
		Items included in 7.1.26 release
		No changes in the current release
		Items included in 7.1.25 release
		No changes in the current release
		Items included in 7.1.24 release
		No changes in the current release
		Items included in 7.1.23 release
RTC 174414		As an ADK for z/OS developer I need to upgrade to OpenSSL 1.0.2o to address PSIRT CVE-2018-0739
		Items included in 7.1.22 release
RTC 52661 RTC 173352	115005	As an AD for z/OS developer I need to offer the ability to explicitly disable TLS1.0 in all ADK based adapters.
RTC 173354	TS000074249	As an ADK for z/OS developer I need to add diagnostic messages to the ADK that allow troubleshooting 2-way ssl connections
RTC 173351		As an ADK for z/OS developer I need to upgrade to OpenSSL 1.0.2n
		Items included in 7.1.21 release
RTC 170056		Include specialFlags in targetprofile.json
		Items included in 7.1.20 release
RTC 163356		Enable SSL by default in the ISPF installation panels
RTC 166577		Add tooltips to customlabels.properties
		Items included in 7.1.19 release
RTC158896	N/A	Status tab in IGI target.json, erLastAccessDate in target.json
RTC156626	N/A	Upgrade expat libraries to 2.2.0
		Items included in 7.1.18 release

RTC154238		Update OpenSSL to release 1.0.2j
RTC154263	PMR 42182,122,000	Disable SSLV3 and RC4 ciphers and certify TLS 1.1 / 1.2 is supported by the ADK
RTC156347	IV32546	Adapter appears to be running while it was unable to connect to the socket.
		Items included in 7.1.17 release
RTC 152024		Include IGI specific profile with JSON in the adapter package
RTC 152027		Update the adapter panels
RTC 152028		Include adapter mapping file in the adapter package
RTC 152030		Include a license folder in the adapter package
RTC 152024		Add two initial lines to CustomLabels.properties which are required for translation
		Items included in 7.0.16 release
RTC 149041		Performance enhancements to the single user account lookup operation.
		Items included in 7.0.13 release
RTC 124240	RFE 67723	ACF2 Password/Passphrase rules used for random password generation
		Items included in 6.0.8 release
		No changes in the current release
		Items included in 6.0.7 release
RTC 116310		Password/pass phrase design independent of password/pass phrase policies.
		Items included in 6.0.6 release
RTC 113711		Add OMVS AUTOUID support
		Items included in 6.0.5 release
RTC 95781		Support for custom boolean attributes defined in the ACFFDR to define additional privileges added.
		Items included in 6.0.4 release
RTC 99347		Support for additional pass phrase and password profile attributes added: PWP-HST PWP-TOD PWPA1TOD PWP-MAXD #PSWDCNT #PWD-TOD KEYFROM
		Items included in release 6.0.3
RTC 98320		Added support for ACF2 pass phrases
		Items included in release 6.0.2
		None

		Items included in release 6.0.1
		ISIM 6.0 release
		Removal of the use of APPC

Closed Issues

Internal#	APAR/CASE#	Description
		Items closed in the current release

RTC 184015	TS002309740	Adapter abend 40D, RC10 with the below messages in the CEEDUMP
		 5 _ermAlloc +00000076 libErmApi.dll
		Call
		   6 ErmSBCSStrtoUCS2Str
		                +000000C0 libErmApi.dll

RTC 184017	TS002309740	Excessive non-ISIM server connections causing abend Starting SSL handshake (OpenSSL)... Handshake failed. Error code: 1 SD_SEND to socket Start SSL cleanup Shutting down SSL server... Received a segmentation violation...
RTC 183205	TS000891911	Debug output in agentCfg tool causes DAML protocol configuration issues
		Items closed in release 7.1.28
RTC 182687		Disallow external calls to agentCfg port
RTC 182516	IJ12296	Reconciliation doesn't return all accounts.
RTC 182686		Upgrade to OpenSSL 1.0.2.q
		Items closed in release 7.1.27
RTC 181308		Upgrade to ICU 3.6
RTC 181306	TS000891911	Hebrew writing direction
RTC 181301		Incorrect entry in adapter log for EXPORT data set
RTC 181302	TS001548171	IKJ56702I INVALID USERID returns error for account DELETE where this should return a success as the account no longer exists in RACF
RTC 181310		Upgrade to Expat 2.2.6
RTC 181303		Upgrade to z/OS ADK 6.0.6
		Items closed in release 7.1.26
RTC 179043		Upgrade to OpenSSL 1.0.2p
		Items closed in release 7.1.25
RTC 177213	TS000991007	Add an option to continue to use tsocmd to allow authorized TSO/E commands to be executed from ISIMEXIT.
RTC 177214	N/A	Invalid status logged for ACF67030: caacf2Adm: success ACF67030 INVALID OPERAND
RTC 177215	TS000934024	ACF2 NAME value corrupted with values from another thread on account ADD
		Items closed in release 7.1.24
RTC 176685		rc > 0 on pre-modify ISIMEXIT doesn't fail the whole operation
RTC 176687	TS000934024	Error for ACF60014 and incorrect name value on account insert
RTC 176690	TS000933551	ISIM ACF2 adapter floods the z/OS consoles (syslog/operlog) with repeating messages for attributes #PSWDCNT and #PWD-TOD
		Items closed in release 7.1.23
RTC 174141	TS000074249	two-way SSL connections don't work – verify errors
RTC 174576	TS000116909	ACF2 adapter 6.0.22 ABEND during account ADD

		Items closed in release 7.1.22
RTC 173353	TS000114491	As an ADK for z/OS developer I need to ensure that manually dropping the DAML_PORT socket doesn't result in a loop
RTC 173360	TS000013259	Since installing 6.0.29 customer cannot longer change the DAML password
RTC 173656	TS000116909	As an adapter for ACF2 developer I need to replace the ACF2 command interface with a higher-performance implementation
RTC 173723		Attempt to destroy context for invalid socket results in dump in _ermListFree
		Items closed in release 7.1.21
RTC 170052	TS000037180	Use configurable HLQ for temporary SYSIN and SYSPRINT
RTC 170053	TS000016341	Adapter returns a failure for informational message ACF6C019
RTC170054	TS000013752	The ACF2 adapter fails with insert error.
RTC170055		PSIRT Malformed X.509 IPAddressFamily could cause OOB read (CVE-2017-3735)
		Items closed in release 7.1.20
RTC 166463	PMR 22742,003,756	RSA key length used by certTool increased from 1024 to 4096, which allows it to be NIST compliant beyond 2021.
RTC 166575	APAR IV98963	IRX0043I Error running ISIMEXIT: TSO/E address space specific functions can't be accessed.
RTC 166576	PMR 23652,999,616	ACF2 single user lookup fails
		Items closed in release 7.1.19
RTC 162836	IV90803	ISIMLUSR reconciliation step fails due to a too small data buffer size. HLQ is not configurable during installation.
RTC 162841	IV90803	findAmap error when an attribute value contained the string "NO". Incorrect year for several PACKDATE attributes. No heapsize _CEERUNOPTS settings predefined.
		Items closed in release 7.1.18
RTC 154265	PMR 08179,999,616	ACF2 adapter delaying due to lack of available threads
RTC 156860		IDMAP delete value request results in modify set value to empty
RTC 156861	IV90803	ACF 2 Adapter - fix from 6.1.16 missing in 6.1.17
		Items closed in release 7.1.17
RTC 134910	N/A	If an account is not defined in the BASE segment, but is in other segments this might result in an error being returned for the previous (in alphabetical order) account being returned during a reconciliation or lookup operation.
RTC 152025		Unknown values PWP-ENC and PWP-LEN appear in ACF2SCHM and ISIMSCHM
RTC 152026		Adapter generates incorrect commands when adding/modifying IDMAP fields for an account
RTC 152342	IV90803	Reconciliation fails when returning data for unsupported segments
		Items closed in release 7.0.16

RTC149785		Sticky bit set for adapter read-only directories
RTC151016	PMR 06782,99,616	Fixed adapter abend that occurs while processing date/time attributes
		Items closed in release 7.0.15
RTC 134666		OpenSSL upgrade to 1.0.1m
RTC 134210	IV78675	Dates are corrupted during reconciliation after changing the account's password.
		Items closed in release 7.0.13
RTC 124038		Updated LREC size to prevent abend "IEF450I TIMA518R ITIMLINF - ABEND=S002 U0000 REASON=00000018 778" when processing large UID strings
		Items closed in release 6.0.8
RTC 122805		Part of long pass phrase is displayed in adapter log
RTC 120578		When setting ACF2 Pass Phrase ACF61003 INVALID KEY returns in logs
		Items closed in release 6.0.7
RTC 116310	IV65077	The adapter does not return daylight savings time based values to the ISIM server.
		Items closed in release 6.0.6
RTC 112239	IV61213	Inconsistent behaviour ACF2 adapter when performing multiple PW changes
		Items closed in release 6.0.5
RTC 95871	IV45874	Custom boolean attributes processing errors
		Items closed in release 6.0.4
RTC 95781	IV45874	Temporary Data set created during reconciliation not cataloged
		Items closed in release 6.0.3
RTC 95781	IV45874	Temporary Data set created during reconciliation not cataloged – Beta fix
		Items closed in release 6.0.2
		Problems with parallel processing
	IV25449	Error in setting the READ_TIMEOUT parameter.
		Items closed in release 6.0.1
		None

Known Issues

INTERNAL#	APAR#	PMR# / Description
	N/A	Random passwords/pass phrases generated by the adapter do not implement site specific GSO Password/Pass phrase policies
	N/A	This release of the CA ACF2 Adapter does not support FIPS.
RTC 52399	N/A	The adapter is designed to read its configuration file on start up. If the configuration file is not found, the adapter will create a new default configuration file. The creation of this configuration file is not an event that is written to the adapter log file. Please ensure TCP/IP is fully initialized and the file systems are mounted before starting the adapter. Under rare conditions where prerequisites for startup have not been met, the adapter may overwrite a customer's configuration file with a new default configuration file.
	N/A	This version of the adapter does not support the following data segments/ user profile records: • DCE • KERB • KERBLINK • KEYRING • LINUX • OPERPARM • MFA

Installation and Configuration Notes

See your products specific ACF2 Adapter Installation and Configuration Guide for detailed instructions.

Configuration

ADK version 6.04 and higher offer a DAML PROTOCOL setting that allows you to disable TLSv1.0. ADK version 6.0.3 and higher no longer support SSLV3 and RC4 ciphers. The ISIM server should be configured to use TLS 1.1 or higher. This is done by adding the $ITIM/data/enRole.properties parameter. For example:

com.ibm.daml.jndi.DAMLContext.SSL_PROTOCOL=TLSv1.1

Possible values are:

TLSv1.1	TLS v1.1 protocol (defined by RFC 4346).
TLSv1.2	TLS v1.2 protocol (defined by RFC 5246).

Corrections to the Installation and Configuration sections of the adapter guide.

Chapter 1: Overview

No updates for the current release

Chapter 2: Planning

No updates for the current release

Chapter 3: Installing

No updates for the current release

Chapter 4: Upgrading

No updates for the current release

Chapter 5: Configuring

No updates for the current release

Chapter 6: Troubleshooting

No updates for the current release

Chapter 7: Reference

No updates for the current release

Starting and stopping the adapter

Before you start the adapter, ensure that TCP/IP is active.

Changing the number of active threads

The CA ACF2 agent requires one process per thread plus 8. The default settings are for 3 threads for each of the four types or requests which is a maximum of 12 active threads which equates to 20 processes (12 + 8). This is below the default MAXUSERPROC value of 25. If you change the maximum thread count variables via agentCfg then you might need to increase the MAXUSERPROC parameter in the parmlib member BPXPRMxx.

Customizing or Extending Adapter Features

The IBM Security Identity 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 CA ACF2 for z/OS adapter has REXX scripting options. Please see the CA ACF2 for z/OS Installation and Configuration guide for additional details.

Support for Customized Adapters

The integration to the IBM Security Identity 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.

IBM Security Identity Product Resources

Check the [Identity and Access Management Products](#) overview.

Supported Configurations

Installation Platform

The IBM Security Identity Manager Adapter supports any combination of the following product versions.

Adapter Installation Platform:
　　　　z/OS V2.2 and higher

Managed Resource:
　　　　CA ACF2 R16

IBM Security Identity Manager:
　　　　Identity Manager v7.X

IBM Security Privileged identity Manager :
　　　　Privileged Identity Manager v2.X

IBM Security Identity Governance and Intelligence:
　　　　IBM Security Identity Governance and Intelligence server v.5.2.X

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
IBM Security Identity Manager

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.

CA, CA ACF2, and CA Top Secret are trademarks of CA, Inc. in the United States, other countries, or both.

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.

ITIL® is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

IT Infrastructure Library® is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

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

End of Release Notes