Release Notes

IBM® Tivoli® Identity Manager

CA ACF2 for z/OS Adapter

Version 5.1.15

First Edition (April 21, 2016)

This edition applies to version 5.1 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 CA ACF2 for z/OS 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 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 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.

Service Groups Management

The ability to manage service groups is a new feature introduced in TIM 5.1. By service groups, TIM is referring to any logical entity that can group accounts together on the managed resource.

Managing service groups implies the following:

Create service groups on the managed resource.
Modify attribute of a service group.
Delete a service group.

Note that service group name change is not supported in TIM 5.1 release.

The CA ACF2 for z/OS adapter does not support service groups management.

Contents of this Release

Adapter Version

Component	Version
Build Date	March 24, 2016
Adapter Version	5.1.15
Component Versions	Adapter Build 5.1.15000 Profile 5.1.1004 ADK 6.02002 z/OS enRole Resource Management API 6.0.2002 OpenSSL 1.0.1m
Documentation	CA ACF2 for z/OS Adapter Installation and Configuration Guide SC23-9617-00

New Features

Enhancement # (FITS)	Description
	Items included in current release
	None
	Items included in 5.1.14 release
	None
	Items included in 5.1.13 release
RTC 124240 RFE 67723	ACF2 Password/Passphrase rules used for random password generation
	Items included in 5.1.12 release
	None
	Items included in 5.1.11 release
RTC 116310	Password/pass phrase design independent of password/pass phrase policies.
	Items included in 5.1.10 release
RTC 113711	Add OMVS AUTOUID support
	Items included in 5.1.9 release
RTC 95781	Support for custom boolean attributes defined in the ACFFDR to define additional privileges added.
	Items included in 5.1.8 release
RTC 99347	Support for additional pass phrase attributes added: PWP-HST PWP-TOD PWPA1TOD PWP-MAXD #PSWDCNT #PWD-TOD KEYFROM
	Items included in 5.1.7 release
RTC 98320	Added support for ACF2 Passphrases
	Items included in 5.1.6 release
	None
	Items included in 5.1.5 release
	Added support for CA ACF2 R15
	Items included in 5.1.4 release
	None

	Items included in 5.1.3 release
MR0702103751	Add User ID to the ITIM Service form (surrogate logonid support)
MR0630103616 MR0902101128 MR1007102414 MR1210105341	Added support for CA ACF2 R14
MR0225113222	ACF2 to be able to parse Close Parenthesis in Data Value
	Items included in 5.1.1 release
	First release of the CA ACF2 for z/OS Adapter.

Closed Issues

Internal#	APAR#	PMR# / Description
		Items included in current release
RTC 141114		PMR 13527,442,000 / “ACFC1199 Command sent to XX nodes" informational message results in error.
		Items included in 5.1.14
RTC 134666		OpenSSL upgrade to 1.0.1m
RTC 134210	IV78675	Dates are corrupted during reconciliation after changing the account's password.
		Items included in 5.1.13
RTC 124038		Updated LREC size to prevent abend “IEF450I TIMA518R ITIMLINF - ABEND=S002 U0000 REASON=00000018 778” when processing large UID strings
		Items included in 5.1.12
RTC 120578		When setting ACF2 Pass Phrase ACF61003 INVALID KEY returns in logs
		Items included in 5.1.11 release
RTC 116310	IV65077	The adapter does not return daylight savings time based values to the ISIM server.
		Items included in 5.1.10 release
RTC 112239	IV61213	Inconsistent behaviour ACF2 adapter when performing multiple PW changes
		Items included in 5.1.9 release
RTC 95871	IV45874	Custom boolean attributes processing errors
		Items included in 5.1.8 release
RTC	IV45874	Temporary Data set created during reconciliation not cataloged

95871		
RTC 99348	IV45874	ISIM ACF2 schema not updated to include PWP-EXP
		Items included in 5.1.7 release
		None
		Items included in 5.1.6 release
		None
		Items included in 5.1.5 release
	IV08078	Warning on account provision reported as error by adapter.
		28339,024,649 The function 'homedir' missing from CA ACF2 adapter ITIMEXIT example user exit.
		28442,024,649 Password expired attribute not checked correctly.
	IV20288	**80913,442,000** Reconciliation fails with unicode attributes returned in attribute names.
		Length error on attributes eracf2MEMLIMIT and eracf2SHMEMMAX. This fix corrects an error to the generated member userid.ITIMACF2.DATA(ACF2SCHM).
		Items included in 5.1.4 release
	AV07154	Duplicate OID values generated in the schema by installation job J8 and conversion routine UpdateACF2OIDs.wsf
		Items included in 5.1.3 release
	IZ79328	UPDATE DOCUMENTATION FOR ACF2 ADAPTER ON CREATING SCHEMA.DSML
	IZ79322	SERVICE PRE-REQUISITE AND OWNER FIELDS DEFINED AS TEXT OBJECT IN THE ACF2 ADAPTER
	IZ86303	RACF AND ACF2 ADAPTER WITH 2-WAY SSL (REGISTER CERTIFICATE). Registered certificates giving 'Subject validation failed' message even when correctly registered.
	N/A	13681,112,848 certTool generating corrupt CSRs
	IZ96327	RESPONSE MESSAGE FOR REQEUST SHOWS A PARSING ERROR. Error: An invalid XML character (Unicode: 0x1a) was found in the value of attribute "matchedDN" and element is "LDAPResult”
		Internal Changes: • Improved ITIMEXIT example. • Change references to ACIDs (Top Secret terminology) to logonids.

		• Minor corrections to installation panels including the generated instructions. • Improve error processing of failed APPC conversations. • Improve error processing of reconciliation - check for security violations of the storage info and fail the whole lot if so as this could lead to incomplete data returned on recon. • Fix a problem where an attribute name containing the string ‘UID’ was being changed to ‘UI$’ causing errors. • Fix problem with passwords being printed in the adapter log. • The tool ACF2PROF that generates the schema from the ACF2 fields now generates object-ids (OIDs) based on the attribute name, to avoid attribute names and OIDs becoming out of synch on subsequent executions of the tool. • Fixed the script that executes certTool, so it references the registry in the correct directory. • Manual changes to the ACF2SCHM table not required any more for the following attributes. NOSPOOL, SYNERR, SECCTL
		Items included in 5.1.1 release
		None

Known Issues

CMVC#	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	**FIPS** This release of the CA ACF2 Adapter does not support FIPS mode.

	N/A	**Read-Only Attributes**
		The CA ACF2 schema is customizable and the list of read-only attributes may be unique for your system. The standard list includes:
		`ACC-CNT      ACC-DATE     ACC-SRCE`
		`CRE-TOD      CSDATE       CSWHO`
		`GRP-USER     HOMENODE     KERBCURV`
		`LID          PSWD-MIX     PSWD-SRC`
		`PSWD-TOD     UID          UPD-TOD`
		`PWP-HST      PWP-TOD      PWPA1TOD`

	N/A	**Unsupported Data Segments**
		This version of the adapter does not support the following data segments:
		`DCE          KERB         KERBLINK`
		`KEYRING      LINUX        OPERPARM`
		`PASSWORD     PROXY`

		Special characters in the attribute names
		Adapter installation generates a schema to be incorporated into the adapter profile, and a matching cross reference table for the adapter task. When generated, the schema and cross reference table files, must be scanned for attribute names containing the following characters ‘-‘, ‘$’ , ‘*’, and those characters must be replaced with an alpha numeric character. The adapter profile will not install correctly if the attribute names contain any of these characters.
		
		So before building and importing the profile you must scan and replace the generated ITIMSCHM for all references of the invalid attribute name. e.g.
		
		`<!-- erAcf2ICLASS*`
		`-->`
		`  <!--`
		`********************************************************`
		`-->`
		`  <attribute-type single-value = "true" >`
		`    <name>erAcf2ICLASS*</name>`
		`    <description>ICLASS-* in segment BASE</description>`
		
		`<object-identifier>1.3.6.1.4.1.6054.3.156.1.120</object-identifier>`
		`  <syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>`
		`  </attribute-type>`

```
…
<attribute ref = "erAcf2ICLASS*" required = "false" />

Replace the ‘*’ with ‘a’

<!-- erAcf2ICLASSa
-->
  <!--
********************************************************
-->
  <attribute-type single-value = "true" >
    <name>erAcf2ICLASSa</name>
    <description>ICLASS-* in segment BASE</description>

<object-identifier>1.3.6.1.4.1.6054.3.156.1.120</object-i
dentifier>
  <syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
  </attribute-type>

…
<attribute ref = "erAcf2ICLASSa" required = "false" />
```

Then the generated cross reference file ACF2SCHM must be updated so the attribute names match. The ACF2 field names must be left untouched. E.g.

```
ICLASS-* erAcf2ICLASS*    BASE     BINARY   S * * 000004
0003
```

should be changed to:

```
ICLASS-* erAcf2ICLASSa    BASE     BINARY   S * * 000004
0003
```

Notes:
-This requires care that attribute names are not duplicated, for example ‘erAcf2ICLASSa’, as used above, may already exist.
- The attribute name length is restricted to 14 characters, so it is advised to replace one character with one character.

Installation and Configuration Notes

See the “IBM Tivoli Identity Manager CA ACF2 Adapter Installation and Configuration Guide” for detailed instructions.

Corrections to Installation Guide

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

Upgrading to 5.1.15

Refer to the Installing and configuring section of the CA ACF2 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 CA ACF2 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.ITIMACF2.CNTL and populates data files in userid.ITIMACF2.DATA.
3. Assuming installing directly over an existing, working adapter with no changes to the installation parameters (the saved variables), then the only installation jobs in data set userid.ITIMACF2.CNTL that need to be submitted are listed below:

   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. You might need to change the disposition of the LOAD and EXEC DD statements to DISP=MOD.

   J8: This job extracts the active ACF2 schema and places it into a flat file which in turn is used as input to create the ITIM schema.dsml file. This job needs to be rerun when upgrading to version 5.1.15.

Note: The member userid.ITIMACF2.EXEC(ITIMEXIT) will be replaced with the new sample ITIMEXIT, so you may wish to make a backup copy of your current ITIMEXIT.

Installing the adapter language pack

See the IBM Security Identity Manager Install library and search for information about installing the adapter language pack.

IBM Security Identity Manager Resources:

Check the “Learn” section of the IBM Security Identity Manager Knowledge Center for links to training, publications, and demos.

Configuration Notes

The following configuration notes apply to this release:

Single account lookup

In release 5.1.14 a new transaction type has been introduced for the reconciliation of a single account using the (eruid=<userid>) filter in ITIM: the LOOKUP transaction.
This transaction ensures that no Pdu entries are created for entries that don't match the eruid specified in the search filter in the server request . For debugging this type of processing more messages for the _ermPduAddEntry process have been added in the Base Logging level (BSE).
Unfiltered requests or requests with more than one account specified in the search filter will still result in a full reconciliation using the standard SEARCH transaction.
To support multiple threads for LOOKUP transactions a new registry setting has been added to the agentCfg tool, which can be configured from the Advanced Settings Menu as depicted below:

```
                  Advanced Settings Menu
         ----------------------------------------------

         A.  Single Thread Agent (current:FALSE)
         B.  ADD max. thread count. (current:3)
         C.  MODIFY max. thread count. (current:3)
         D.  DELETE max. thread count. (current:3)
         E.  SEARCH max. thread count. (current:3)
         F.  LOOKUP max. thread count. (current:3)
         G.  Allow User EXEC procedures (current:FALSE)
         H.  Archive Request Packets (current:FALSE)
         I.  UTF8 Conversion support (current:TRUE)
         J.  Pass search filter to agent (current:FALSE)

         X.  Done

         Select menu option:
```

Timezone support

The adapter converts all date values to UTC before forwarding them to the ITIM server. The adapter uses the $TZ timezone variable specified in the environment settings for the adapter account (e.g. ITIAGNT) to specify the offset it should use to convert the local timezone to UTC. When no offset is specified the adapter will assume the received date can be returned as UTC without any further conversion.
So for instance the TZ definition in /etc/profile or the adapter account specific profile should be TZ=EST5, or TZ=EST5EDT for daylight savings time, rather then TZ=EST.

OMVS AUTOUID support

The ITIM RACF Adapter 5.1.10 and above supports auto-assignment of OMVS UIDs using AUTOUID.
To define a user for which the OMVS UID should be auto-assigned by ACF2 type the word 'AUTOUID' (case sensitive) in the attribute field on the ITIM server account form for that user.
When receiving a numeric userid value from the ITIM server, the adapter will execute the following command: INSERT <USER> UID(<NUMERIC VALUE>)

Example:
'INSERT IBMUSER UID(2345)'

When receiving the string AUTOUID from the ITIM server, the adapter will execute the following command: INSERT <USER> AUTOUID

Example:
'INSERT IBMUSER AUTOUID'

Password Phrases

ITIM ACF2 Adapter 5.1.8 and above support ACF2 pass phrases. A pass phrase in ACF2 is an authentication mechanism that allows the secret string to be between 9 and 100 characters. While setting passwords from the IBM Tivoli Identity Manager server, a string lesser than or equal to eight characters is treated as a password and a string more than eight characters is treated as a pass phrase.

Starting the current ISIM Adapter version 5.0.13 the implementation of random password and pass phrase generation has changed. Random passwords and pass phrases will be generated using a configuration string which determines the type and number of characters to be generated.
The default built-in string for passwords is: an$NaANa
The default built-in string for pass phrases is: an$NaANa#aaNAa
The password generator will generate passwords as follows:

- for every occurrence of A, the adapter will randomly generate a letter from A-Z
- for every occurrence of a, the adapter will randomly generate a letter from a-z
- for every occurrence of N (uppercase!), the adapter will randomly generate a numeric from 0-9
- for any other character (including lowercase n), the adapter will simply echo that character back

Internally the adapter will ensure it will not generate the same characters consecutively.
The built-in strings can be modified using new registry settings:
PWD_CONFIG for password configuration strings
PWP_CONFIG for pass phrase configuration strings

PWD_CONFIG will allow a maximum of five (5) comma-separated strings which will be randomly selected by the adapter to generate random passwords.
The size of each string should be between 5 and 8 characters long. In the event a shorter string is specified the adapter will report an error and try another string. In the event a longer string is specified the adapter will use only the first 8 characters to generate a password.
The configuration string is not allowed to contain any of the following hard-coded reserved words:

```
ACF,APPL,APR,ASDF,AUG,BASIC,CADAM,DB2,DEC,DEMO,ENT,FEB,FOCUS,GAME,IBM,IMS,JAN,
JUL,JUN,LOG,MAR,MAY,NET,NEW,NOV,OCT,OTIS,PASS,ROS,SEP,SIGN,SONI,SYS,TEST,TSO,T
SYS,VALID,VTAM,WELC,XXXX,0000,1111,1234,222,3333,4444,5555,6666,7777,8888,9999
,',"
```

In the event a reserved word is found in the configuration string the adapter will report an error.
After receiving an error the adapter will attempt to select another random configuration string. After two failed attempts the adapter will stop processing and return an error.
The adapter will consider the first four characters of the logonid for the request it is currently processing as a reserved word. In other words: the adapter will also report an error in the event the first four characters of the logonid are part of the configuration string. Reserved word and short logonid validation is case insensitive.
Reserved word and short logonid validation is repeated for the generated password. In the event the adapter detects a reserved word and/or short logonid as part of the generated password the adapter will stop processing and return an error.
A new registry setting allows specifying additional reserved words: RESWORD.
Any comma-separated string found in the RESWORD registry setting value will be added to the hard-coded reserved words list during request processing.

PWP_CONFIG will allow a maximum of three (3) comma-separated strings which will be randomly selected by the adapter to generate random password phrases.
The adapter requires the size of each string to be between 9 and 100 characters long, the string should however be at minimum as long as the minimal length specified in the ACF2 Password phrase rules. In the event a string of less then 9 characters is specified the adapter will report an error and try another string. In the event a string of more then 100 characters is specified the adapter will use only the first 100 characters to generate a password phrase.
The configuration string is not allowed to contain single or double quotes.
In the event a single or double quote is found in the configuration string the adapter will report an error.
After receiving an error the adapter will attempt to select another random configuration string. After two failed attempts the adapter will stop processing and return an error.

For information on how to add and modify registry settings please refer to section “Modifying non-encrypted registry settings” of Chapter 4 “Configuring the Adapter for IBM Security Identity Manager”
in the Adapter Installation and Configuration Guide.

Other password phrase related registry settings

In the ITIM Adapter version 5.1.12 additional registry settings for pass phrase have been introduced.
Support for additional registry settings has been implemented to allow customization of the actions to be taken when using the ITIM Adapter to set pass phrases using the password field on the ITIM Server.
For information on how to add and modify registry settings please refer to section “Modifying non-encrypted registry settings” of Chapter 4 “Configuring the Adapter for IBM Tivoli Identity Manager”
in the Adapter Installation and Configuration Guide.

Registry setting for changing phrases:
PASSGEN=ADD (generate random password on ADD account with pass phrase)
PASSGEN=MOD (generate random password on MODIFY account with pass phrase)
PASSGEN=NEVER (never generate a random password)
PASSGEN=BOTH (always generate a random password)

If not specified PASSGEN will default to BOTH
Note: IBM does not guarantee the random passwords generated will meet the site specific password rules.

Registry settings for changing passwords:

1. PWPMOD = RANDOM (generate a random phrase on MODIFY account with password)
2. PWPMOD=DISABLE (will not generate a random phrase, but rather disables pass phrase usage for this LID on MODIFY account with password)
3. PWPMOD=IGNORE(no changes are made for the pass phrase when the request is for changing a password)

If not specified PWPMOD will default to RANDOM.
Note: IBM does not guarantee the random pass phrases generated will meet the site specific pass phrase rules.

Note: With PASSGEN set to NEVER or MOD new accounts can only be requested using a password. When attempting to add a new account using a pass phrase with PASSGEN set to NEVER or MOD the following error will be returned:
ERR:yy/mm/dd hh:mm:ss caacf2Add: pass phrases can NOT be used for INSERT for user <LID>

Since PWPMOD=DISABLE will ensure pass phrase usage for a specified LID is disabled on account MODIFY when changing a password for this LID an additional registry setting has been introduced to specify if PWPALLLOW should automatically be re-enabled when receiving a request to set a pass phrase for a LID.
1. AUTOPWP=TRUE (automatically set PWPALLOW when receiving a request to change a pass phrase)
2. AUTOPWP= FALSE (don't automatically set anything for the phrase when the request is for changing a phrase)

If not specified AUTOPWP will default to TRUE

Make sure that the ACF2 requirements for pass phrases are included in the IBM Tivoli Identity Manager server rules for passwords. This includes setting the minimum characters in the password string to be more than 8 in the password policy. If the rules for password phrases employed at your installation site is not reflected in the Tivoli Identity Manager server password policies, then there is a possibility of ACF2 rejecting the entered pass phrase.

In the existing documentation, all references to an ACF2 password now encompass both ACF2 passwords and pass phrases.

Custom boolean attributes

The adapter has been changed to support custom boolean attributes defined as either <PRIVILEGENAME> when privilege is granted to a user or as NO<PRIVILEGENAME> when the user has not been granted the privilege. E.g. MYCICS or NOMYCICS specified for a specific ACF2 logonid.

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 CA ACF2 for z/OS Adapter also has REXX scripting options. Please see the CA ACF2 for z/OS Adapter 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

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

Operating System:
z/OS V1.13.X
z/OS V2.1.X
z/OS V2.2.X

Managed Resource:
CA ACF2 R14
CA ACF2 R15
CA ACF2 R16

IBM Tivoli Identity Manager:
Identity Manager v5.1

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

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.

End of Release Notes