Release Notes

IBM® Tivoli® Identity Manager

Authentication Manager (ACE) Adapter

Version 5.0.4

First Edition (February 3, 2011)

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 RSA Authentication Manager (ACE) 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 RSA Authentication Manager (ACE) Adapter Installation and Configuration Guide

Adapter Features and Purpose

The RSA ACE Adapter is designed to create and manage accounts on Authentication Manager. The adapter runs in “agent” mode and must be installed on the Authentication Manager server. The adapter communicates using the ACE API to the systems being managed.

The adapter must be installed on the Authentication Manager (ACE) system being managed. A single copy of the adapter can handle one Identity Manager Service. 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.

Contents of this Release

Adapter Version

Component	Version
Release Date	February 3, 2011
Adapter Version	5.0.4
Component Versions	Adapter Build 5.0.1014 Profile 5.0.1001 ADK 5.19
Documentation	RSA Authentication Manager Adapter for Windows Operating Systems Installation and Configuration Guide SC23-6167-00

New Features

Enhancement # (FITS)	Description
	Items included in current release
MR111710511	Ace 6.1 adapter modified to support users imported from LDAP See “Configuration Notes” for additional information.
	Items included in 5.0.2 through 5.0.3 release
	None
	Items included in 5.0.1
	Initial release for Tivoli Identity Manager v5.0

Closed Issues

CMVC#	APAR#	PMR# / Description
		Items closed in current version
	IZ85960	61075,227,000 ACE Adapter may crash when received the modify request for attribute without the value.
		Items closed in 5.0.3 version
	IZ33132	08848,057,649 Sequential modify request failed for all attribute of user, after rename operation.
		Items closed 5.0.2 version
	IZ09724	22492,L6Q Reconciliation process may crash if no Tokens (supporting data) are returned.

Known Issues

CMVC#	APAR#	PMR# / Description
N/A	N/A	Editing adapter profiles on UNIX or Linux. The adapter profile JAR file may contain ASCII files created using MS-DOS ASCII format (i.e. schema.dsml, CustomLabels.properties, and service.def). If you edit a MS-DOS ASCII file in Unix you will often see the characters ^M at the end of each line. This is the extra character 0x0d that is used to indicate a new line of text in MS-DOS. There are tools, such as dos2unix, that can be used to strip out the ^M character. In addition, there are text editors that will ignore the ^M character. If you are using the vi editor, you can strip out the ^M character as follow: From the vi's command mode: :%s/^M//g followed by pressing Enter. The ^M (or Ctrl-M) typed to show it here should actually be entered by pressing ^v^M in sequence. (The ^v preface tells vi to use the next keystroke literally instead of taking it as a command.)
N/A	N/A	Event Notification of Groups During event notification, add request for GroupEntries with length of more than 120 characters are created but ADK fails to insert the entry into Event Notification Data Base.
N/A	N/A	Event Notification Account status (Active/Inactive) might not be correctly updated on Identity Manager after event notification.
		This adapter does not use an xforms.xml file. Errors in the adapter log concerning xforms may be safely ignored. Error message is: "Unable to load XML transformation buffer from...".
		Class 3 Certificate Installation Class 3 Certificates (class 3 secure server CA-G2) are not written properly to “DamlCACerts.pem” file through CertTool.exe Utility. The certificate data is written twice between BEGIN CERTIFICATE and END CERTIFICATE. **Work around:** To correct this issue, please follow the below steps and edit “DamlCACerts.pem” file present in “<Adapter installation path>\data” folder. **Step 1.** Start the CertTool utility **Step 2.** Import the class 3 CA certificate by using “F” option from the main menu of CertTool Utility. **Step 3.** Once the class 3 CA certificate is successfully installed, open

		"DamlCACerts.pem" file stored in the "<Adapter installed path>\data" folder using text editor. **Step 4.** Delete the class 3 CA certificate data (i.e. content between BEGIN CERTIFICATE and END CERTIFICATE) from "DamlCACerts.pem". **Step 5.** Open class 3 CA certificate file using text editor and copy the certificate data (between the BEGIN CERTIFICATE and END CERTIFICATE) **Step 6.** Paste the certificate data to "DamlCACerts.pem" file between the BEGIN CERTIFICATE and END CERTIFICATE lines of same class 3 CA Certificate. If more than one class 3 certificates are installed then you can identify the certificate using issuer and subject data. **Step 7.** Save "DamlCACerts.pem" file. **Step 8.** To verify the "DamlCACerts.pem" file is edited properly, display certificate information by using option "E" from the main menu of CertTool Utility. **Note:** Please note that this issue is seen after installing class 3 CA certificate. If you correct the DamlCACerts.pem and then install another class 3 CA certificate, the newly installed class 3 CA certificate will show same issue. This issue is also seen when you delete any certificate using option "G" from the main menu of CertTool utility. The delete option will affect all remaining class 3 CA certificate and you have to follow step 1 to 8 to correct the DamlCACerts.pem file.

Installation and Configuration Notes

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

Running v4.6 and v5.0 Adapters on the Same Server

The Identity Manager version 5.0 adapters have enhanced capabilities that are not compatible with older version 4.6 adapters. It is highly recommended that all adapters hosted on an individual server are upgraded at the same time.

Adapters installed on the same server may share common components or run-time environments. The version 4.6 adapters may not be compatible with the version 5.0 component and may no longer operate as expected after installation of a version 5.0 adapter. On Windows servers all adapters must be upgraded simultaneously due to the sharing of DLLs. Check the adapter installation guide for additional information.

Corrections to Installation Guide

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

None

Configuration Notes

The following configuration notes apply to this release:

NOTE: The account, which the Agent will run from, must comply with the following:

- The Agent account must have full permissions on the directory that contains the ACE/Server software.
- The Agent account must be registered in the ACE/Server database with administrator role.

Maximum Token Limit:

The ACE/Server limits the number of tokens to three. When assigning a password to a user, the ACE/Server will treat that as a special token, hence, the available numbers of tokens will become two.

Assigning Password:

When applying (assigning) a Password to a user, the Agent must receive the following:

a) The password, passed in the Password attribute.
b) Duration of the password is valid, passed in two attributes:
   - Days attribute (number of days password is valid).
   - Duration attribute (number of hours password is valid).
c) PasswordToken attribute MUST be set to YES.

Suspend/Restore a User:

Suspending a user implies that all the user's tokens will be disabled.
Restoring a user implies that all the user's tokens will be enabled.

Using the User Extension Data Feature

The user extension data is a key-data pair and must follow these conventions:

Key: Name for the extension data field. The key can be up to 48 characters.
If key contains a colon (":") then it must be escaped with "\".
The key may not contain " , " as this sequence is used by Ace Server while returning
The key-data pair.

Data: Data that you want to store in this field. The value can be up to 80 characters.

Format: The key-data pair must be separated by ":"
Example "key1:value1" where key=key1 and data=value1.

MR111710511: Ace 6.1 adapter modified to support users imported from LDAP

Prior to this enhancement, wwhen there is a Modify request for a user imported from LDAP the following error occurs:

Sd_SetTempUser Error Cannot change temporary state for user synchronized from LDAP.

- During the modify operation for a User ,the API Sd_SetTempUser is called if one of the following attributes are changed
  Temporary User (eracetempuser)

Start Date (eracetmpusrstdt)
End Date (eracetmpusrenddt)

- This API is used to set the modified values for above attributes on the resource.
- However, when the Temporary user flag, Start date or End date for a User imported from LDAP is modified, the API Sd_SetTempUser gives the Error “Cannot change temporary state for user synchronized from LDAP.” The API works fine for non-LDAP users.
- So it is basically a API issue , ideally the behavior of the API should have been the same , irrespective of whether the user has been imported from LDAP or not. Therefore, the above mentioned attributes cannot be modified for users imported from LDAP.

- This issue is fixed by bypassing the call to the API Sd_SetTempUser, when there is no request to modify the Temporary user flag, Start date or End Date. However note that if during a modify request if we explicitly try to modify the attributes Temporary user, start date or end date then the API will be called and the error “Cannot change temporary state for user synchronized from LDAP” will occur. And this is the expected behavior because even on resource it is not possible to modify the Temporary User flag, Start date and End Date for users imported through LDAP.
- But unlike before, this error will not occur if any other attributes (like First name, Last name, Shell etc) is modified.

Note: For Users imported from LDAP, the following attributes cannot be modified.
- Temporary User (eracetempuser)
- Start Date (eracetmpusrstdt)
- End Date (eracetmpusrenddt)

MR0310092030: Support to set new PIN for token. Support to set token in new PIN mode. Support to set PIN to Next Tokencode. PMR 00713,998,649 - Generating the PIN for ACE adapter.

1. Setting a new PIN for the token:
   You can set a new PIN for a token assigned to the user.

   Usage:
   -> The user can specify this value in the 'Set a new PIN' field on the TIM UI. The user can find this field in all
   the token tabs available on the TIM account form.
   -> The user can assign this new pin during the ADD or the MODIFY operation.

2. Setting the token in new PIN mode:

   You can set the token in new PIN mode. In this mode, the user initially authenticates with the Passcode generated by the PIN. On successful logon he/she is prompted for change in PIN. This PIN can be system generated or user defined. Then onwards, user has to login with the Passcode generated by the New PIN.
   Usage:
   ->The user can set the token in New PIN mode from the TIM UI by selecting the field 'New Pin mode’. The user can find this field in all the token tabs available on the TIM account form.
   ->The user can set the token in New PIN mode during the user ADD or the MODIFY operation

3. Setting the PIN to Next Tokencode

You can set a PIN for a token to next tokencode. It means that, the PIN can be set with the first n digits of a next tokencode. To achieve this, you have to provide the Current Tokencode with setting the token to Next Tokencode. Then, you will get the number of digits to be used as PIN from the Next Tokencode.
Usage:
The PIN can be set in Next Tokencode only during the user MODIFY operation.
The following are the steps that the user has to follow for setting the PIN in Next Tokencode.
[1]Note down current tokencode (for example, "12345678") and next tokencode (for example, "87654321") pair for any time period displayed on RSA SecurID Token Device UI
[2]The user has to select the 'Set PIN to Next Tokencode' checkbox on the TIM UI.
[3]The user has to type the noted current token code to the field 'Current Tokencode' on the TIM UI. For example, Current Tokencode is "12345678".
[4]The new PIN of the token will be the first n digits of the Next Tokencode. For example, Next Tokencode is "87654321".

Then, the user has to send a reconciliation/lookup request from the TIM UI. After performing the reconciliation/lookup request, the user is able to see the value of field 'Number of digits to be used from the Next Tokencode as PIN' on the same token tab. For example, "4".
Then, the user will be able to login to the resource with the new PIN i.e. The new PIN will be the first n (For example, 4 is the number of digits seen in the field 'Number of digits to be used from the Next Tokencode as PIN') digits of the Next Tokencode that has been noted down. For example, "8765" will be the new PIN for the token as these are the first 4 digits of the Next Tokencode "87654321".
The user request for setting the PIN in Next Tokencode will fail if the Next Tokencode starts with 0. This is resource behavior.

Notes:
--After the PIN is set in Next Tokencode successfully, the user will find a new user extension data of the type ITIMToken=<Token_number> : <no of digits>. For example, "ITIMToken=101010101: 4". The user is requested not to change or delete this data, since it is used by the adapter.
--The removal of this user extension data is handled by the adapter appropriately during token assignment.
--The user may also find a change in the User extension data, when he sets the PIN in Next Tokencode successively.

MR0615102351 - Need all dates managed by the ACE adapter to be handled in the same date format ,that is, Zulu).

For more details refer the configuration notes section "Retrieving the token related attributes Value in Zulu or Ace Server local format ".
Following items needs to be added to "Configuration Notes" in release notes.

- **Retrieving the token related attributes value in Zulu or Ace Server local format.**

Below are the date type attributes managed by ace adapter.

Sr.No	Attribute	Label on TIM side	Reconciled only (R) Add/Mod permit(W)
1	eracetmpusrstdt	Start Date	W

2	eracetmpusrenddt	End Date	W
3	erAceToken1ActivationDate	Date Activated(Token#1)	R
4	erAceToken1ShutdownDate	Date Will Shutdown (Token#1)	R
5	erAceToken1EnableDisableDate	Date Enabled/Disabled (Token#1)	R
6	erAceToken1LastLoginDate	Last Login Date (Token#1)	R
7	erAceToken2ActivatedDate	Date Activated (Token#2)	R
8	erAceToken2ShutdownDate	Date Will Shutdown (Token#2)	R
9	erAceToken2EnableDisableDate	Date Enabled/Disabled (Token#2)	R
10	erAceToken2LastLoginDate	Last Login Date (Token#2)	R
11	erAceToken3ActivatedDate	Date Activated (Token#3)	R
12	erAceToken3ShutdownDate	Date Will Shutdown (Token#3)	R
13	erAceToken3EnableDisableDate	Date Enabled/Disabled (Token#3)	R
14	erAceToken3LastLoginDate	Last Login Date (Token#3)	R
15	erAcePasswdActivatedDate	Date Activated (Special Token)	R
16	erAcePasswdShutdownDate	Date Will Shutdown (Special Token)	R
17	erAcePasswdEnableDisableDate	Enabled/Disabled (Special Token)	R
18	erAcePasswdLastLoginDate	Last Login Date (Special Token)	R

The eracetmpusrstdt and eracetmpusrenddt were already managed by adapter in the Zulu format.

To support this enhancement added new registry key “DATE_FORMAT_IN_ZULU” in the adapter. The expected value will be TRUE or FALSE. Initially default value will be FALSE.

1. DATE_FORMAT_IN_ZULU = TRUE
   - If you set the registry key value to TRUE, then during reconciliation or user Lookup operation the date type attributes value related to the tokens will be return to TIM in Zulu (YYYYMMDDHHMMZ i.e. 201007251021Z) format.
   - Note: - In Zulu time format seconds will be ignored.

2. DATE_FORMAT_IN_ZULU = FALSE
   - If you set the registry key value to FALSE, then during reconciliation or user Lookup operation the date type attributes value related to the tokens will be return to TIM in Ace Server local (MM/DD/YYYY HHH:MMM:SSS i.e. 07/24/2010 000:000:000) format.

To modify the value of registry key "DATE_FORMAT_IN_ZULU" use agentcfg tool.

- **Setting the Start Date and End Date value through ITIM.**
  Following Scenarios should be consider to avoid loss of minutes from erAceTmpUsrStDt "Start Date" and
  erAceTmpUsrEndDt "End Date" attributes while setting them from ITIM Side.
  All the scenarios listed below are applicable to EndDate also.

1. If time zones of ITIM and Ace Server are same
   A. If ITIM and Ace Server time zones are GMT +/– **X: 00**
   For example: - ITIM and Ace Server time zones are GMT - 05:00
   You must set minutes as 0(refer case 1 from Table 1).
   If you do not set minutes as 0 then adapter will set it as 0 on Ace Server (refer case 2 from Table 1).

Case no.	ITIM Time Zone	Date set from ITIM MM/DD/YYYY	ACE Server Time Zone	Date set on Ace Server UI MM/DD/YYYY	Time show on TIM UI after reconciliation MM/DD/YYYY
1	GMT - 5	Start Date 04/06/2010 06.00 PM	GMT - 5	04/06/2010 18.00	04/06/2010 06.00 PM
2	GMT - 5	Start Date 04/06/2010 06.30 PM	GMT - 5	04/06/2010 18.00	04/06/2010 06.00 PM

Table 1

   B. If ITIM and Ace Server time zones are GMT +/– **X: 30**

   For example: - ITIM and Ace Server time zones are GMT + 05:30
   You must set minutes as 0 (refer case 1 from Table 2).
   If you do not set minutes as 0 then adapter will set it as 0 on Ace Server (refer case 2 from Table 1).

Case no.	ITIM Time Zone	Date set from ITIM MM/DD/YYYY	ACE Server Time Zone	Date set on Ace Server UI MM/DD/YYYY	Time show on TIM UI after reconciliation MM/DD/YYYY
1	GMT + 5:30	Start Date 04/06/2010 05.00 AM	GMT + 5:30	04/06/2010 05.00	04/06/2010 05.00 AM
2	GMT + 5:30	Start Date 04/06/2010	GMT + 5:30	04/06/2010 05.00	04/06/2010 05.00 AM

		05.30 AM			

Table 2

2. If time zones of ITIM and Ace Server are different
   A. If ITIM time zone is GMT +/– **X: 00** and Ace Server time zone is GMT +/– **Y: 00**
   For example, ITIM time zone is GMT - 05:00 and Ace Server time zone is GMT + 06:00 you must set
   minutes as 0(refer case 1 from Table 3).

   If you do not set minutes as 0 then adapter will set it as 0 on Ace Server (refer case 2 from Table 3).

Case no.	ITIM Time Zone	Date set from ITIM MM/DD/YYYY	ACE Server Time Zone	Date set on Ace Server UI MM/DD/YYYY	Time show on TIM UI after reconciliation MM/DD/YYYY
1	GMT - 5	Start Date 04/06/2010 06.00 PM	GMT + 6	04/07/2010 05.00	04/06/2010 06.00 PM
2	GMT - 5	Start Date 04/06/2010 06.30 PM	GMT + 6	04/07/2010 05.00	04/06/2010 06.00 PM

Table 3

   B. If ITIM time zone is GMT +/– **X: 30** and Ace Server time zone is GMT +/– **Y: 30.**
   For example, ITIM time zone is GMT - 5:30 and Ace Server time zone is GMT + 6:30 you must set
   minutes as 0(refer case 1 from Table 4).

   If you do not set minutes as 0 then adapter will set it 0 on Ace Server (refer case 2 from Table 4).

Case no.	ITIM Time Zone	Date set from ITIM MM/DD/YYYY	ACE Server Time Zone	Date set on Ace Server UI MM/DD/YYYY	Time show on TIM UI after reconciliation MM/DD/YYYY
1	GMT - 5:30	Start Date 04/06/2010 4.00AM	GMT + 6:30	04/06/2010 16.00	04/06/2010 04.00 AM
2	GMT - 5:30	Start Date 04/06/2010	GMT + 6:30	04/06/2010 16.00	04/06/2010 04.00 AM

		4.30AM			

Table 4

C. If ITIM time zone is GMT +/– **X: 00** and Ace Server time zone is GMT +/– **Y: 30.**
For example, ITIM time zone is GMT - 5:00 and Ace Server time zone is GMT + 6:30 you must set minutes as 30(refer case 1 from Table 5).
If you do not set minutes as 30 then you will get minutes as 30 during reconciliation from Ace Server (refer case 2 from Table 5).

Case no.	ITIM Time Zone	Date set from ITIM MM/DD/YYYY	ACE Server Time Zone	Date set on Ace Server UI MM/DD/YYYY	Time show on TIM UI after reconciliation MM/DD/YYYY
1	GMT - 5:00	Start Date 04/06/2010 05.30 AM	GMT + 6:30	04/06/2010 17.00	04/06/2010 05.30 AM
2	GMT - 5:00	Start Date 04/06/2010 05.00 AM	GMT + 6:30	04/06/2010 16.00	04/06/2010 04.30 AM

Table 5

D. If ITIM time zone is GMT +/– **X: 30** and Ace Server time zone is GMT +/– **Y: 00.**

For example, ITIM time zone is GMT - 5:30 and Ace Server time zone is GMT + 6:00 you must set minutes as 30(refer case 1 from Table 6).
If you do not set minutes as 30 then you will get minutes as 30 during reconciliation from Ace Server (refer case 2 from Table 6).

Case no.	ITIM Time Zone	Date set from ITIM MM/DD/YYYY	ACE Server Time Zone	Date set on Ace Server UI MM/DD/YYYY	Time show on TIM UI after reconciliation MM/DD/YYYY
1	GMT - 5:30	Start Date 04/06/2010 05.30 AM	GMT + 6:00	04/06/2010 17.00	04/06/2010 05.30 AM
2	GMT - 5:30	Start Date 04/06/2010 05.00 AM	GMT + 6:00	04/06/2010 16.00	04/06/2010 04.30 AM

Table 6

Troubleshooting

The following troubleshooting notes apply to this release:

Following items needs to be added to “RSA Authentication Manager Adapter for Windows Operating Systems Installation and Configuration Guide”

Chapter 9 .Troubleshooting.

Error message	Possible Cause	Corrective action
Sd_SetTempUser Error Cannot change temporary state for user synchronized from LDAP	This error occurs if modification operation is requested for the following attributes 1. Temporary User (eracetempuser) 2. Start Date (eracetmpusrstdt) 3. End Date (eracetmpusrenddt) for users imported from LDAP.	Following attributes cannot be modified for users imported from LDAP. 1. Temporary User (eracetempuser) 2. Start Date (eracetmpusrstdt) 3. End Date (eracetmpusrenddt)

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.

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:
Windows 2003

Managed Resource:
RSA Authentication Manager v6.1

IBM Tivoli Identity Manager:
Identity Manager v6.1

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.

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