

Release Notes



IBM[®] Tivoli[®] Identity Manager

Active Directory 64-Bit (WinAD64) Adapter

Version 4.6.5

First Edition (March 3, 2009)

This edition applies to version 5.0 of Tivoli Identity Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Copyright International Business Machines Corporation 2003, 2008. All rights reserved.
US Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP
Schedule Contract with IBM Corp.

Contents

Preface.....	4
Adapter Features and Purpose	4
Contents of this Release	5
Adapter Version.....	5
New Features	6
Closed Issues	8
Known Issues	11
Installation and Configuration Notes	15
Running v4.6 and v5.0 Adapters on the Same Server.....	15
Corrections to Installation Guide.....	15
Configuration Notes.....	15
Exchange 2007 and Exchange 2003 in Co-Existence Mode	15
Deleting a Mailbox.....	16
Directory NTFS and Share Access	16
Expiration Date.....	16
Password Properties.....	16
Setting Language Preference for Accounts.....	16
Log Message: Error More Data	16
Use SSL Configuration Option	17
Use Default DC Configuration Option	17
Use new Win2003 ADSI API for managing WTS attributes	18
Win AD Agent handle Add and Delete operations for erGroup attribute	18
Support for LastLogonTimeStamps Attribute	18
Remote Access Permission Attribute	19
Upgrading from TIM v4.6 Profile	19
Solving Replication Delay while Adding Mailbox on Exchange 2007	20
Using DN or GUID for the ergroup Attribute	20
Managing the Dial-in, Callback Settings, and Callback Number	23
Single Transaction for Modifying Mail-user to Mailbox User	23
Support for Windows 2008.....	23
Registry option: ReconMailboxPermissions	24
Home directory security attributes.....	24
Failover of Target Systems – Multiple Servers in Basepoint.....	24
Proxy Address Attribute Change/Delete.....	25
Provisioning to Child Domain - UPN Checking	26
Note:	27

Improve primary group lookup using cache	27
Customizing or Extending Adapter Features.....	28
Getting Started	28
Support for Customized Adapters.....	28
Supported Configurations.....	29
Installation Platform	29
Notices	30
Trademarks	31

Preface

Welcome to the IBM Tivoli Identity Manager Active 64-bit Directory (WinAD64) 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 Active Directory Adapter with 64-Bit Support Installation and Configuration Guide

Adapter Features and Purpose

The Active Directory Adapter is designed to create and manage accounts on Microsoft Active Directory. The adapter runs in “agentless” mode and communicates using Microsoft ADSI API and PowerShell (for exchange communication) to the systems being managed.

IBM recommends the installation of this adapter in “agentless” mode on a 64-bit OS and computer in the domain being managed. Installation on a Domain Controller is not recommended. A single copy of the adapter can handle multiple Identity Manager Services. 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	March 2, 2009
Adapter Version	4.6.5 (v5.0.6)
Component Versions	Adapter Build 5.0.1019 64-bit Profile 5.0.1010 ADK 5.11 64-bit
Documentation	Active Directory Adapter with 64-bit Support Installation and Configuration Guide SC23-9479-00 Active Directory Adapter with 64-bit Support User Guide SC23-9480-00 Password Synchronization for Active Directory Plug-in Installation and Configuration Guide SC23-6178-00

New Features

Enhancement # (FITS)	Description
	Items included in current release
WARNING	<p>WinAD64 is a new adapter designed to support AD and Exchange 2007.</p> <p>WinAD64 is not an upgrade of the WinAD Adapter. While the objectClass names have remained the same as WinAD to ease the migration to this new adapter, it is important that customers review all TIM Policies and retest all third-party integrations. The features of the WinAD and WinAD64 adapters are not identical due to changes in the underlying Microsoft components.</p>
MR0212084734	Enhancement to handle failover of target systems by supporting multiple target servers in basepoint.
MR0831085255	Management of field msRADIUSFramedIPAddress in Active Directory
N/A	Improve primary group lookup performance using cache.
	Items included in 5.0.5 release
MR0808084336	Add support for Exchange 2007 attribute 'msexchrequireauthntosendto'.
MR0825086415	Enhance the adapter to allow an account to be changed from a mail-user to a mailbox user in a single transaction.
N/A	<p>Add support for Windows 2008 as a target AD.</p> <p>Add support for Windows 2008 as a host platform for the adapter.</p>
	Items included in 5.0.2 release
MR0825086415	AD adapter profile modified to include the DL e-mail attribute.
MR121707567	Modified the adapter to accept a single MODIFY operation to change a user from mail-user to mailbox user.

Enhancement # (FITS)	Description
	Items included in 5.0.2 release
MR0427076459	Enhance adapter to support the AD LastLogonTimeStamp attribute. See “LastLogonTImeStamp Attribute” in the configuration section of this document for more information.
MR1118053029	Enhance the adapter to support all options of the RemoteAccessPermission property. See “Remote Access Permission Attribute” in the configuration section of this document for more information.
	Items included in 5.0.1 release
MR0302076050	WinAD: support for Exchange 2007 by TIM v4.6.
MR0625072952	WinAD: AD Adapter needs to support Exchange 2007.
MR0709074515	WinAD: TIM 4.6 needs adapter to support Exchange 2007
MR082107737	WinAD: Exchange 2007 adapter support needed.
MR1017076035	WinAD: the Active Directory adapter needs to support Exchange 2007

Closed Issues

CMVC#	APAR#	PMR# / Description
		Items closed in current version
	IZ38367	59070,082,000 Adapter provisioning to child domain UPN issue. NOTE: the adapter will now check that the UPN is unique within the Forest.
	IZ42815	67170,650,706 WinAD Adapter installer issue if the path contains a space.
	IZ44751	57426,004,000 ITIM WinAD 64 Bit Crash.
	IZ40688	49313,379,000 null attrs in Exch 07 issue WINAD64 bit Adapter.
33974		N/A WinAD Adapter recon returning unwanted exchange attributes.
33977		N/A WinAD64 attribute erADEProxyAddresses to be sent as add-delete
34278		N/A WinAD64 ADprofile update. Corrected jar format that prevented successful import to TIM.
		Items closed in 5.0.5 version
	N/A	Updated the PW Sync Plug-In 1) MR1017081822 - create a version of PW Sync without 3rd party dependencies 2) PMR 37512,379,000 - Added more logging in domain bind and user lookup. 3) 77327,021,724 - Code changes for ignoring TIM response when TIM application is down Down
	IZ35340	CertTool crashes for ADAGENT on Win 64-bit.
		Items closed in 5.0.4 version
	IZ35901	35389,379,000 erADEHideFromAddrsBk in AD 64bit Agent needs to return either TRUE or FALSE value during recon (for a mail-user or mailbox user).
	IZ35932	16714,7TD,000 AD Adapter recon fails because the recon event crashes the service when parsing security descriptor data for a user it recons.

CMVC#	APAR#	PMR# / Description
		Items closed in 5.0.3 version
33182	N/A	Values for "Reject Mail From" and "Delegates" are not cleared on the resource, though Agent reports success for requests to clear the values of these attributes.
33183	N/A	Agent doesn't retrieve correct value of exchange attribute 'Permanent delete only after backup' through recon on Windows 2003 64bit AD.
33188	N/A	Setting Forwarding Style as "Recipient or Forward", the attribute "deliverAndRedirect" should be set to "false". But the attribute's value gets cleared.
N/A	N/A	Windows AD Adapter 64bit crashes on Windows 2008 64bit when neither Exchange Server 2007 nor PowerShell is installed.
		Items closed in 5.0.2 version
	IZ24107	37721,550,000 WinAD Adapter returns success for add request with home directory creation, but the home directory is not created on the resource
	IZ13159	19535,005,000 Enhancement to support the third dial-in option "Control access through Remote Access Policy"
	IZ25019	65296,001,822 Problem with setting the 'erlogontimes' attribute to 'Mid-Hour'. The adapter throws an error expecting a 168 bit string. Documentation change : AD Adapter erLogonTimes can only be set to hourly and not to 'Mid-Hour'.
	IZ24750	42485,999,866 AD Password Sync plug-in 5.0.1 does not check the origin of password change.
	IZ23735	70262,379,000 Replication delay leads to an error while adding mailbox on Exchange 2007.
	IZ30086	84473,379,000 WinAD64 creating unwanted proxy addresses during account creation with alias specified.

CMVC#	APAR#	PMR# / Description
32850	N/A	N/A Issue adding user to groups in Windows 64-bit AD agent.
32557	N/A	N/A AD Agent sets WTS drive letter instead of WTS Home directory in "Local path" on AD.
32558	N/A	N/A WinAD Adapter returns success but cn is not set on AD. Attributes mobile, postofficebox, givenname, sn, telephonenumber, street, pager, l, mail, homephone, postalcode, title, description and st are send as add-delete for a modify request instead of replace.
32579	N/A	N/A WinAD wrongly sets Dialin Callback option as "Set by caller (Routing and Remote Service only)" when "Fixed callback number" is selected.
		Items closed in 5.0.1 version
		None

Known Issues

CMVC#	APAR#	PMR# / Description
N/A	N/A	<p>Failed transaction when changing UserName and Alias</p> <p>PMR 83090,379,000 describes a situation where replication delays within AD may cause a rename action to fail if BOTH the AD account and the Exchange mailbox are changed in the same operation.</p> <p>For now the work-around is to complete the renaming in two steps: Step 1 - Rename non-exchange attributes (CN, displayName, givenName, samAccountName - eruid, etc.). Step 2 - Rename exchange attributes (Mailbox Alias).</p>
N/A	N/A	<p>Editing adapter profiles on UNIX or Linux.</p> <p>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.</p> <p>If you are using the vi editor, you can strip out the ^M character as follow: From the vi's command mode:</p> <pre>:%s/^M//g</pre> <p>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.)</p>

CMVC#	APAR#	PMR# / Description														
		<p><i>Issues with Adapter installed on Windows 2003 64bit and managing Active Directory on Windows 2003 64bit or Windows 2008</i></p> <p>1. Known Issues for Enhancement to support the third dial-in option "Control access through Remote Access Policy"</p> <p>1) In mixed-mode domain functional level third dial-in option "Control access through Remote Access Policy" is not supported. If an attempt is made to set dial-in as "Control access through Remote Access Policy" agent will report attribute level failure to TIM, but on the resource dial-in will be set to "Deny Access" (default). If previously dial-in was set to "Allow Access" after the above failed request dial-in will be set as "Deny Access".</p> <p>Workarround: No workaround available.</p> <p>2) Reconciliation on mixed mode domain functional level shows incorrect value "Control access through Remote Access Policy" for Dial-in attribute for accounts created directly on Active Directory with the combination "Deny Access" (Dial-in) and "No Callback" (Callback option).</p> <p>There are two cases when Active Directory does not create attribute msNPAllowDialin as shown in below table.</p> <table><tr><th>Domain Functional Level</th><th>Attribute Value on Active Directory</th></tr><tr><td>Windows 2000 Native</td><td>Dial in: Control access through Remote Access Policy Callback options: No Callback (default)</td></tr><tr><td>Windows 2000 Mixed</td><td>Dial in: Deny Access (default) Callback options: No Callback (default)</td></tr></table> <p>During search, active directory does not return attribute msNPAllowDialin and also adapter can not find the functional level of domain without connecting to RootDSE. Connecting to RootDSE does not work if you have installed adapter in domain other than one you are managing. So adapter sets erADExDialin as "NONE", which is "Control access through Remote Access Policy" on account form.</p> <p>Work around:</p> <p>If you want to retrieve correct value then while creating user directly on Active Directory, set following as defaults instead of "No Callback" for Callback option.</p> <table><tr><th>Attribute</th><th>Value</th></tr><tr><td>-----</td><td>-----</td></tr><tr><td>Dialin</td><td>Deny Access</td></tr><tr><td>Callback Options</td><td>Set by caller</td></tr></table>	Domain Functional Level	Attribute Value on Active Directory	Windows 2000 Native	Dial in: Control access through Remote Access Policy Callback options: No Callback (default)	Windows 2000 Mixed	Dial in: Deny Access (default) Callback options: No Callback (default)	Attribute	Value	-----	-----	Dialin	Deny Access	Callback Options	Set by caller
Domain Functional Level	Attribute Value on Active Directory															
Windows 2000 Native	Dial in: Control access through Remote Access Policy Callback options: No Callback (default)															
Windows 2000 Mixed	Dial in: Deny Access (default) Callback options: No Callback (default)															
Attribute	Value															
-----	-----															
Dialin	Deny Access															
Callback Options	Set by caller															

CMVC#	APAR#	PMR# / Description
N/A	N/A	Using the Upgrade Option: The Upgrade option is applicable only to 5.0.x maintenance upgrades. The upgrade option is not designed for v4.6 to v5.0 migrations. NOTE: After using "Update Installation" option with higher version of Adapter, an extra folder with name "_uninst2" is created. It can be ignored. To Uninstall the Adapter, use "_uninst" folder.
N/A	N/A	Event Notification Account status (Active/Inactive) might not be correctly updated on Identity Manager after event notification.
N/A	N/A	Event Notification "Adapter Based" event notification is not supported in this release.
N/A	N/A	N/A The User ID field cannot contain a "," (comma).
		IMPORTANT NOTE: The BasePoint (on Service form) and the Event Notification Context (in agentCfg) must be in proper DN format. All special characters must be escaped.
N/A	N/A	PMR 83403,057,649 - AD Agent hangs on second error Work around implemented for Microsoft issue (KB article 293278). For user add request, the agent binds to the basepoint/default domain and checks to see if the specified user already exists. Each operation is run in a separate thread which first initializes COM using CoInitialize and upon operation completion calls CoUninitialize to uninitialize COM. However for second request, the connection is reused and agent quickly establishes connection with AD. MS KB article 293278 (http://support.microsoft.com/default.aspx?scid=kb;en-us;293278) states that 'PRB: Problems When You Call CoInitialize and CoUninitialize Repeatedly in Multithreaded Apartment' - To avoid the issue, a small delay (1 sec) has been inserted before COM is uninitialized at the end of operation. This delay is ONLY applicable when 'User already exists' condition is encountered and DOES NOT affect any other functionality.

CMVC#	APAR#	PMR# / Description
N/A	N/A	<p>Below is list of TIM AD adapter attributes and corresponding attribute in Active Directory</p> <p>erADLastFailedLogin -> badPasswordTime erADBadLoginCount -> badPwdCount erADLastLogoff -> lastLogoff erADLastLogon -> lastLogon</p> <p>The above attributes are nonreplicated attribute, which means that each domain controller holds its own copy of the attribute, likely with different values.</p> <p>The WinAD adapter may not show actual value for these attributes.</p>

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:

Configuration Notes

The following configuration notes apply to this release:

Note that the “supported configurations” diagrams have been moved into the Installation Guide.

Exchange 2007 and Exchange 2003 in Co-Existence Mode

The WinAD64 adapter supports Exchange 2007/2003 co-existence mode but Microsoft lists several important limitations. The adapter enforces these same limitations (see Microsoft link below).

- Exchange 2007 mailboxes must be managed with Exchange 2007 management console or shell.
- Exchange 2007 mailboxes MUST NOT be managed with Exchange 2003 tools. Note that this is not blocked, but mailboxes managed from Exchange 2003 ADUC will not be fully functional.
- Exchange 2003 mailboxes can be edited or removed with Exchange 2007 tools, but cannot be created by Exchange 2007 tools.
- Both Exchange 2003 and Exchange 2007 mailboxes can be moved (in either direction) with the Exchange 2007 tools. Exchange 2003 move mailbox cannot be used to move mailboxes to or from Exchange 2007 mailbox server.

Based on the above restrictions, the WinAD64 adapter has the following capabilities:

- Exchange 2007 mailboxes can be full managed
- Exchange 2003 mailboxes can only be modified. Attempts to create a 2003 mailbox will fail.

WARNING: The WinAD64 adapter is not designed to convert mailboxes to 2007 format.

While it is possible for the WinAD64 adapter to move a mailbox from a 2003 mailbox to a 2007 mailstore, doing so will cause a conversion of the mailbox. The conversion may cause the TIM transaction to time out. Converting mailboxes is not a supported function of the WinAD64 adapter; use the Exchange 2007 tools to convert mailboxes.

For additional Exchange information, please refer to Microsoft web-based resources:

<http://msexchange team.com/archive/2006/10/09/429135.aspx>

Deleting a Mailbox

To delete a Mailbox, delete the Mailbox Store attribute. Submit a reconciliation request to clear unnecessary values from the account form and to verify that the mailbox has been removed.

Directory NTFS and Share Access

The Agent returns the actual, effective permissions granted to a user and not the specific access assigned to the user account. For example, if the directory grants FULL permission to the Everyone group but only CHANGE permission to the user's account, a reconciliation request will return the account access permission as FULL. Therefore, it is necessary to properly define the policies local to the managed resource prior to using Tivoli Identity Manager to prevent these types of conflicts.

Expiration Date

Per Microsoft's documentation, the Active Directory Users and Computers MMC snap-in will display the account expiration date as one day earlier than the date contained in the accountExpires attribute. The Tivoli Identity Manager Server will display the value contained in the account expires attribute.

Password Properties

The password properties are specific to the account. However, these properties can be overridden by the security policies of the managed resource (Domain Controller Security Policies, Domain Security Policies, and Local Security Policies).

Setting Language Preference for Accounts

The Languages attribute (eradlanguage) is an Exchange attribute. If using a configuration without Exchange, setting this attribute will return a warning.

Log Message: Error More Data

NOTE: If a Reconciliation is run while the Active Directory server is under load, a logging message may appear in the WinAD Adapter log that says, "Error_More_Data." The Adapter is designed to retry the query three times before terminating the Reconciliation. Please see the Microsoft Knowledge base article below for more information.

When the IDirectorySearch::GetNextRow function returns S_ADS_NOMORE_ROWS, it may not have retrieved all the data from the server. In some cases, S_ADS_NOMORE_ROWS is returned by GetNextRow function when the server was unable to find an entry that matched the search criteria within a predefined two-minute time limit. This two-minute time limit is defined by means of an LDAP policy.

If the server exceeds the two-minute time limit, it returns an LDAP cookie in the response so that you can restart the search where it left off. Inefficient searches and heavily loaded systems can cause the server to exceed the time limit. When the server cannot find an efficient index to search, the server may have to apply the filter to every object in the directory, in which case it can run through many entries and not find a match within the two-minute time limit.

Therefore, when returning S_ADS_NOMORE_ROWS, ADSI also sets an extended error code, which can be queried using ADsGetLastError function. If ADsGetLastError returns ERROR_MORE_DATA, it means that the server has not completed the query and must call GetNextRow again.

The AD Agent code is structured as per the logic above and what Microsoft has advised. It attempts to get data from the paged result in max 3 attempts. If the AD Agent is running on AD server itself, Moving the AD Agent onto a different machine would take off some load from AD server.

In addition to this Microsoft has provided an article as how to configure the LDAP policy so as to customize the Active Directory searches. <http://support.microsoft.com/kb/315071/EN-US/>.

Use SSL Configuration Option

The registry setting “useSSL” is to enable SSL communicating between AD Agent and Active Directory. If TRUE, agent communicates over SSL with Active Directory. If this key is not present or FALSE, agent does not use SSL.

By default this key is set to FALSE. No ITIM side changes are required to use this enhancement.

Following resource side changes are required to use this feature.

- a. Active Directory must have enabled Public Key Infrastructure (PKI). For this Enterprise Certificate Authority should be installed on one of the domain controller machine in the domain. Setting up an enterprise certificate authority causes an Active Directory server to get a server certificate that can then be used to do SSL-based encryption.
- b. Machine on which AD Agent is running should have certificate installed. The certificate is issued by CA as mentioned in point (a).

Use Default DC Configuration Option

The useDefaultDC registry setting is to provide failover capability to agent when host specified in base point is down. If agent is unable to connect to hostname specified in base-point and key is set to TRUE, agent will connect to the base-point without the host name. If it still fails then agent will report failure. By setting this key to TRUE also affects behavior of RAS server and Terminal server lookup.

Caution: When the adapter is deployed in a cross-domain scenario, the useDefaultDC option should always be set to FALSE to avoid provisioning to an unintended domain. For example, if the adapter is installed in domain A but provisioning to domain B, and the host in domain B is down, the adapter will detect the default domain as domain A.

By default this key is set to FALSE.

The behavior of agent will be as follows:

A. useDefaultDC = FALSE

- i. If hostname (target server name) is specified in the base point and ForceRASServerLookup and ForceTerminalServerLookup registry keys are set as FALSE, then agent uses the given hostname as RAS server and Terminal server.
- ii. If hostname (target server name) is specified in the base point and ForceRASServerLookup and ForceTerminalServerLookup registry keys are set as TRUE, then agent will determines the RAS and Terminal server name.

B. useDefaultDC = TRUE and host is down.

- i. Agent will determines RAS and Terminal server irrespective of values set for ForceRASServerLookup and ForceTerminalServerLookup.

Use new Win2003 ADSI API for managing WTS attributes

Agent will use WTS ADSI API's or old style WTS API's to set or retrieve WTS attributes. Agent will try to use WTS ADSI API's, if it fails to get interface or attribute is not supported then agent will use old style WTS API's.

If agent is running on Windows 2003 then agent will use WTS ADSI API's. On Windows 2000 agent will use old style WTS API's.

From log it can be found out which WTS API's agent is using. Some of the attributes are not supported by WTS ADSI API's; for that agent will use old style WTS API's on Windows 2000 and Windows 2003.

If debug logging is enabled, then agent will show lines like:

- ☐ *Start using extended interface for WTS Attributes for getting WTS attribute.*
- ☐ *Start using extended interface for WTS Attributes for setting WTS attribute.*
- ☐ *End using extended interface for WTS Attributes for setting WTS attribute.*
- ☐ *End using extended interface for WTS Attributes for getting WTS attribute.*

This means agent is using WTS ADSI API's.

If log is showing lines like:

- ☐ *Using old style API for WTS Attributes for getting WTS attribute*
- ☐ *Using old style API for WTS Attributes for setting WTS attribute*

This means agent is using old style WTS API's.

Win AD Agent handle Add and Delete operations for erGroup attribute

WinAD Adapter by default honors only replace operation from Tivoli Identity Manager. WinAD Adapter now supports Add and Delete operation for erGroup attribute for Modify request.

On Tivoli Identity Manager profile changes are required in ADprofile to send group operation as add, delete for modify request.

See the steps below

- Locate the following line in resource.def file under <Operation Name="modify"> tag.

```
<Parameter Name="erGroup" Source="account" ReplaceMultiValue="true" />
```

- Replace the above line with following line.

```
<Parameter Name="erGroup" Source="account" />
```

- Reinstall the profile. Please see Windows Active Directory Adapter Install guide for further references.

Support for LastLogonTimeStamp Attribute

This version of Windows Active Directory Adapter supports lastLogonTimeStamp attribute of Active Directory. Attribute lastLogonTimeStamp is available on Windows 2003 domain functional level and is replicated. The default replication interval is 14 days, but some customers have increased this frequency so that the attribute can be used as a basis for Dormant Account reporting.

To support this enhancement, the profile of Windows Active Directory Adapter is extended. A new Date attribute erADLastLogonTimeStamp (OID: 1.3.6.1.4.1.6054.3.125.2.146) is defined and added in erADAccount class. A new label (eradlastlogontimestamp=Last Login Time Stamp) is added to CustomLabels.properties file.

Note: The attribute erADLastLogonTimeStamp is not visible on account form. To bring it on account form, form customization is required.

Remote Access Permission Attribute

Windows Active Directory Adapter has Boolean attribute "erADAllowDailin" to represent msNPAllowDialin. As attribute "erADAllowDialin" is Boolean and can not be used to represent three values, Windows Active Directory Adapter schema is extended. A new String attribute "erADEXdialin" (OID: 1.3.6.1.4.1.6054.3.125.2.145) is added in erADAccount class.

Attribute "erADEXdialin" is added to the Windows Active Directory Adapter account form (erADAccount.xml). Following new labels are added to CustomLabels.properties file.

eradexdialin=Dial-in
tag.dialin.allow=Allow Access
tag.dialin.deny=Deny Access
tag.dialin.none=Control access through Remote Access Policy

The account form now has a combo box instead of a checkbox representing one of the three values for dial-in. The default value is "Deny Access".

Value displayed on account form	Value sent in request and stored in TIM LDAP
Allow Access	TRUE
Deny Access	FALSE
Control access through Remote Access Policy	NONE

NOTE:

1. Attribute "erADAllowDailin" is deprecated and removed from the account form. It will not be processed by adapter.
2. If you have any business logic around attribute "erADAllowDialin" then you must modify it to use "erADEXdialin".

Upgrading from TIM v4.6 Profile

(applicable only for customers using profile shipped with Adapter build 4.6.1024)

If you are using profile which is shipped with Windows Active Directory Adapter build 4.6.1024, following changes required in IBM Tivoli Identity Manager LDAP schema.

In release 4.6.1024, following attribute was added:

erADEXdialin 1.3.6.1.4.1.6054.3.125.2.138

In WinAD64-4.6.0 & WinAD64-5.0.1, following 7 new attributes are added :

erADEAllowedAddressList	1.3.6.1.4.1.6054.3.125.2.138
erADEOutlookWebAccessEnabled	1.3.6.1.4.1.6054.3.125.2.139
erADEActiveSyncEnabled	1.3.6.1.4.1.6054.3.125.2.140
erADEMAPIEnabled	1.3.6.1.4.1.6054.3.125.2.141

erADEEnableRetentionHold	1.3.6.1.4.1.6054.3.125.2.142
erADEStartRetentionHold	1.3.6.1.4.1.6054.3.125.2.143
erADEEndRetentionHold	1.3.6.1.4.1.6054.3.125.2.144

If you are using profile shipped with Windows Active Directory Adapter version 4.6.22 (adapter build 4.6.1024), then importing Windows Active Directory Adapter (64-bit) schema will not create attribute erADEAllowedAddressList.

Change erADExDialin OID to 1.3.6.1.4.1.6054.3.125.2.145 in Windows Active Directory Adapter schema and add it to the Windows Active Directory Adapter (64-bit) schema. Henceforth OID 1.3.6.1.4.1.6054.3.125.2.145 OID used in default Windows Active Directory Adapter schema.

You must perform the following schema changes prior to installing this version:

1. Stop the IBM Tivoli Identity Manager Server.
2. Stop the IBM Tivoli Directory Server Instance (LDAP service).
3. Locate the V3.modifiedschema file under the ITIM LDAP instance home directory.
4. Create a backup of the V3.modifiedschema file, for example V3.modifiedschema.backup.
5. With a text editor, open the V3.modifiedschema file and locate the "1.3.6.1.4.1.6054.3.125.2.138" string.
6. Replace "1.3.6.1.4.1.6054.3.125.2.138" with "1.3.6.1.4.1.6054.3.125.2.145"
7. Save the file V3.modifiedschema and exit the editor.
8. Restart the IBM Tivoli Directory Server Instance (LDAP service).
9. Restart the IBM Tivoli Identity Manager Server.

Solving Replication Delay while Adding Mailbox on Exchange 2007

On exchange 2007 when creating a mailbox or mail enable a user during its creation, an error may be returned from Active Directory saying the user does not exist. This is because of a delay in replication among the DCs. Because of this replication delay, Exchange may not find an account on a DC if it is other than the one on which the account is created.

If you encounter this error while creating mailbox or mail-enable an user, then specify the Base Point on service form along with target server on IBM Tivoli Identity Management Server for Active Directory Adapter service. Specifying a Base Point will ensure that the adapter uses the same DC for both the user creation in AD and the Exchange mailbox request. The Base Point must contain the name of the Domain Controller.

Example

Base Point DN: DC01/ou=Test,dc=MyDomain,dc=com.

Using DN or GUID for the ergroup Attribute

Windows Active Directory Adapter has been enhanced to support Group DN and Group GUID values for erGroup attribute. With this enhancement, multiple groups with the same name that are present in different organizational units on active directory can be processed by the adapter.

Beginning with this version of the adapter, the new registry key "UseGroup" is introduced. The default value for this key is CN. The registry key value can be set to CN or DN or GUID as per the requirement.

Configuration required for using this feature: Perform the following steps (steps A through D):

- A. Set the UseGroup registry key to CN or DN or GUID using agentCfg.
- B. Change the profile files "erADAccount.xml" and "resource.def" Find the table below describing what change need to be done when UseGroup registry value is set to CN or DN or GUID

Find the table below describing what change need to be done when UseGroup registry value is set to CN or DN or GUID

Use Group value	Change required in
CN It is default value	erADAccount.xml <pre> <formElement name="data.ergroup" label="\$ergroup"> <searchFilter multiple="true" type="select"> <filter>(objectclass&#61;eradgroup)</filter> <base>contextual</base> <attribute>eradgroupcn</attribute> <sourceAttribute>eradgroupcn</sourceAttribute> <size></size> <objectClass></objectClass> <showQueryUI>>false</showQueryUI> <paginateResults>>false</paginateResults> </searchFilter> </formElement> </pre> Resource.def <pre> <ServiceGroups> <GroupDefinition ProfileName="ADGroupProfile" ClassName = "erADGroup" RdnAttribute = "erADGroupGUID" AccountAttribute = "erGroup"> <AttributeMap> <Attribute Name="erGroupId" Value="erADGroupCN" /> <Attribute Name="erGroupName" Value="erADGroupCN" /> <Attribute Name="erGroupDescription" Value="description" /> </AttributeMap> </GroupDefinition> </ServiceGroups> </pre>
DN	erADAccount.xml <pre> <formElement name="data.ergroup" label="\$ergroup"> <searchFilter multiple="true" type="select"> <filter>(objectclass&#61;eradgroup)</filter> <base>contextual</base> <attribute>eradgroupdn</attribute> <sourceAttribute>eradgroupdn</sourceAttribute> <size></size> <objectClass></objectClass> <showQueryUI>>false</showQueryUI> <paginateResults>>false</paginateResults> </searchFilter> </formElement> </pre> Resource.def <pre> <ServiceGroups> <GroupDefinition ProfileName="ADGroupProfile" ClassName = "erADGroup" RdnAttribute = "erADGroupGUID" </pre>

	<pre> AccountAttribute = "erGroup"> <AttributeMap> <Attribute Name="erGroupld" Value="erADGroupDN" /> <Attribute Name="erGroupName" Value="erADGroupDN" /> <Attribute Name = "erGroupDescription" Value="description" /> </AttributeMap> </GroupDefinition> </ServiceGroups> </pre>
GUID	<p>erADAccount.xml</p> <pre> <formElement name="data.ergroup" label="\$ergroup"> <searchFilter multiple="true" type="select"> <filter>(objectclass&#61;eradgroup)</filter> <base>contextual</base> <attribute>eradgroupdn</attribute> <sourceAttribute>eradgroupguid</sourceAttribute> <size></size> </objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement> </pre> <p>Resource.def</p> <pre> <ServiceGroups> <GroupDefinition ProfileName="ADGroupProfile" ClassName = "erADGroup" RdnAttribute = "erADGroupGUID" AccountAttribute = "erGroup"> <AttributeMap> <Attribute Name="erGroupld" Value="erADGroupGUID" /> <Attribute Name="erGroupName" Value="erADGroupDN" /> <Attribute Name = "erGroupDescription" Value="description" /> </AttributeMap> </GroupDefinition> </ServiceGroups> </pre>

NOTE:

- 1) The value of the "attribute" tag of the formElement "data.ergroup" in erADAccount.xml should match with the value of "erGroupName" in resource.def.
- 2) The value of the "sourceAttribute" tag of the formElement "data.ergroup" in erADAccount.xml should match with the value of "erGroupld" in resource.def
- 3) Keep the value of the "sourceAttribute" tag of the formElement "data.eradprimarygroup" unchanged to "eradprimarygrptkn". This value has to remain unchanged for CN, DN or GUID support.

- C. Build the ADprofile.jar and import the new profile into TIM
- D. Run a full reconciliation.

NOTE: If an event notification is enabled, delete the event notification data base using the agentCfg (Refer Install guide for the deleting the event notification database) and then run a full reconciliation. This will make sure that new database get created with correct values for attribute "erGroup"

Managing the Dial-in, Callback Settings, and Callback Number

Attributes Dial-in, Callback Settings, and Callback Number will not be set. These attributes are reconciled properly only if Windows Active Directory Adapter is running as a service and is remotely managing Active Directory. The issue is reproducible on Windows 2003 x64 and Windows 2008 x64 as remote managed platform. The Windows API fails to retrieve the Dial-in attributes.

A workaround for this issue is same as that given for the DevTrack issue (S17341) (APAR# IY84890). That is to set the Dial-in Attributes, specify the user credentials having administrator authority (under which the Agent service runs) in 'Tivoli Active Directory Adapter' Windows service's Properties window.

- 1) Open Windows Services Tool. (i.e. the application, services.msc).
- 2) Go to 'Tivoli Active Directory Adapter' service. Open its Properties window.
- 3) Go to 'Log On' tab, change the default Log On option from 'Local System account' to 'This account'. And specify the Administration user credentials information.
- 4) Restart the 'Tivoli Active Directory Adapter' service.

Single Transaction for Modifying Mail-user to Mailbox User

This version of Windows Active Directory Adapter provides an enhancement to modify a mail account from its existing mail status (e.g. Mailuser) to other mail status (i.e. Mailbox user) in one single ITIM Modify operation. In the earlier versions of WinAD adapter, to modify the mail status, one has to delete the existing mail status in one operation and create the new mail status in another operation.

- To modify a Mailuser account to a Mailbox account -- Clear the target address and specify mailbox store. You may modify the Alias if required. The mailuser status is removed and a mailbox is created for the account.
- To modify a Mailbox account to a Mailuser account -- Clear the mailbox store and specify target address. You may modify the Alias if required. The mailbox is deleted from the exchange and the account is mail-enabled.

NOTE : If Alias is not modified during the above operations, then the Alias value is retained in the new mail status. To delete an existing mail status (mailuser or mailbox) of an account, delete the corresponding attribute, i.e. Mailbox store or Target address. (this behavior is same as previous versions of Adapter). Also once the mail status change operation completes, submit a user lookup operation to clear unnecessary attribute values from the account form so as to avoid warnings for those non-applicable attributes of the new mail status.

All other exchange related operations will work same like in earlier versions of Windows active directory adapter.

Support for Windows 2008

When you use Windows 2008 as a installation platform, and require to run adapter in SSL mode, then follow below steps. Otherwise, the certificate install will not be complete and will not enable SSL correctly.

1. Disable UAC security (User Account Control).
2. Install the required Certificate.
3. If required, enable UAC security.

For more information visit the link to enable/disable the UAC.

http://en.wikipedia.org/wiki/User_Account_Control

Registry option: ReconMailboxPermissions

The registry key, 'ReconMailboxPermissions' is set to TRUE by default. So, by default mailbox security permissions attributes will get reconciled. However, you might experience a crash while reconciling mailbox permissions attributes. So, in that case to skip reconcile of mailbox permissions attributes, set the registry key 'ReconMailboxPermissions' to FALSE, which also improves reconciliation performance.

Attributes corresponding to the mailbox security permissions are:

- Delete Mailbox Storage
- Read Permissions
- Change Permissions
- Take Ownership
- Full Mailbox Access
- Associated External Acc
- Apply Onto (Allow / Deny)
- Permissions inheritance to one level (Allow / Deny)

Home directory security attributes

Note that for the following attributes, if the user neither has FULL nor CHANGE (Modify) access specified on the home directory, then reconciliation will display a blank option on the IBM Tivoli Identity Manager account form.

- Home Directory NTFS Access
- WTS Home Directory NTFS Access
- Home Directory Share Access
- WTS Home Directory Share Access

Failover of Target Systems – Multiple Servers in Basepoint

MR0212084734 – Enhancement to handle failover of target systems by supporting multiple target servers in basepoint.

This version of Windows Active Directory Adapter supports more than one target servers in the base point.

The earlier versions of WinAD adapter supported only one target server for the basepoint. If the specified target server is down and useDefaultDC is set to FALSE, adapter used to fail the request.

With this enhancement more that one target servers can be specified for basepoint on Tivoli Identity Manger's Active Directory Service Form and/or in the Windows Active Directory Adapter's registry. Each target server must be separated by a pipe '|'.

Usage Example,

Base Point DN on service form with more than one target server:
DC01|DC02|DC03/OU=TestOU,DC=MyDomain,DC=com

Base Point DN on service form with only one target server:
DC01/OU=TestOU,DC=MyDomain,DC=com

Base Point DN on service form with no target server:
OU=TestOU,DC=MyDomain,DC=com

Also, target servers can be specified in Adapter's registry as well:

a) If BasePoint specified on service form is "OU=TestOU,DC=MyDomain,DC=com", you can specify the list of target server(s) in adapter registry using agentCfg.exe as follows:

1. Create WinAD adapter registry with name OU=TestOU,DC=MyDomain,DC=com

2. Specify the value for the above key as DC01|DC02|DC03

Registry key	Value
--------------	-------

OU=TestOU,DC=MyDomain,DC=com	DC01 DC02 DC03
------------------------------	----------------

b) If BasePoint specified on service form is

"DC01|DC02|DC03/OU=TestOU,DC=MyDomain,DC=com", you can specify the list of target server(s) in adapter registry using agentCfg.exe as follows:

3. Create WinAD adapter registry with name OU=TestOU,DC=MyDomain,DC=com

4. Specify the value for the above key as DC01|DC02|DC03

Registry key	Value
--------------	-------

OU=TestOU,DC=MyDomain,DC=com	DC01 DC02 DC03
------------------------------	----------------

Adapter iterates through all the target servers specified in base point on service form, and then through the target servers specified in registry key. The first available target server is used by the adapter. You can also wish to specify the base point without the target server(s) on service form, and use the registry key to specify the target servers. Adapter uses the base point specified on the service form to find a key with this base point value in the registry, to get the target servers specified as the value for this registry key.

Note:

1. The maximum number of characters that the Base Point DN attribute on service form can hold is 240 characters.
2. Service form and registry can specify their own set of target servers, the target servers specified on service form is given high priority.

Example,

Base Point on service form

DC01|DC02|DC03/OU=TestOU,DC=MyDomain,DC=com

Registry

Registry key	Value
--------------	-------

OU=TestOU,DC=MyDomain,DC=com	DC04 DC05 DC06
------------------------------	----------------

3. If no base point is specified on service form, the registry will not be referred.
4. It is recommended that you specify target server using adapter's registry as it is cached to improve performance as against specifying on service form. The target server list on service form is not cached and is parsed in each request to find all target servers.
5. Use agentCfg.exe to create and modify adapter registry keys, please restart the adapter service after adding or modifying registry keys. If the basepoint or target server contains Unicode characters then use regedit to create registry keys under HKEY_LOCAL_MACHINE\SOFTWARE\Access360\ADAgent\Specific

Proxy Address Attribute Change/Delete

MR032609161- WinAD Enhancement to handle erADEProxyAddresses attribute in add/delete as well as in replace format.

This version of Windows Active Directory Adapter is enhanced to support erADEProxyAddresses attribute values in an ADD\DELETE format.

Using the current profile, IBM Tivoli Identity Manager will send the erADEProxyAddresses attribute in the modify request with operation type as replace. In order to use this enhancement it is required that the adapter receives the erADEProxyAddresses attribute in the modify request in an add/delete format. The following changes are required in ADprofile.jar so that IBM Tivoli Identity Manager handle the erADEProxyAddresses attribute in add/delete format.

The profile JAR file, ADprofile.jar, is included in the Active Directory Adapter compressed file that you downloaded from the IBM Web site.

Complete the following steps to modify the ADprofile.jar file:

1. Copy the ADprofile.jar file to a temporary directory, for example C:\Temp folder.
2. Extract the contents of ADprofile.jar file into the temporary directory by running the following command:

```
cd C:\Temp
jar -xvf ADprofile.jar
```

The jar command will create the "C:\Temp\ADprofile" directory which will have all the profile files.
3. For Editing ADprofile complete the remaining steps below
 - I. [For editing WinAD Adapter profile for IBM Tivoli Identity Manager version 4.6](#)
 - a) Open xforms.xml file found in the extracted ADprofile folder in text pad.
 - b) Add the following entry between the tags <EnRoleTransformations> and </EnRoleTransformations>

```
<EnRoleAttribute Name="erADEProxyAddresses"
RemoteName="erADEProxyAddresses" ConvertReplaceToAddDelete="true" />
```
 - c) Save the xforms.xml file
 - II. [For editing WinAD Adapter profile for IBM Tivoli Identity Manager version 5.0](#)
 - a) Open resource.def file found in the extracted ADprofile folder in text pad.
 - b) Search for the entry <Parameter Name="erADEProxyAddresses" Source="account" ReplaceMultiValue="true" /> in resource.def file.
 - c) Delete all the occurrences of the above entry from resource.def file.
 - d) Save the resource.def file.
4. Use following commands to create new jar file

```
cd C:\Temp
jar -cvf ADprofile.jar ADprofile
```
5. Import the new ADprofile.jar file into IBM Tivoli Identity Manager Application server. For more information on importing the file, see section "Importing the adapter profile into the Tivoli Identity Manager server" in WinAD Adapter Installation and Configuration guide.
6. After importing the profile, stop and start the Tivoli Identity Manager server to reflect the changes.

Provisioning to Child Domain - UPN Checking

IZ38367 - Adapter provisioning to child domain UPN issue.

This version of Windows Active Directory Adapter provides an additional check for uniqueness of the User Principal Name (UPN) within a forest, while creating a user account.

The adapter now performs search on User Principal Name (which is either generated by the adapter or supplied in the user add request) in the forest to ensure that no two users have same User Principal Name. For this adapter performs a search first in the current managed domain and then in the forest.

Note:

The Current version of adapter does not perform User Principal Name (UPN) check for modify operation.

A new registry key "UPNSearchEnabled" is introduced to use this enhancement. This registry key is set to TRUE by default.

When registry key UPNSearchEnabled is set to FALSE, adapter will not perform a search on User Principal Name for uniqueness and will create the user account with the supplied or generated value of User Principal Name.

When registry key UPNSearchEnabled is set to TRUE, adapter works as follows:

Case 1: User Principal Name is supplied in the user add request.

Adapter will use the value of User Principal Name and will perform a search. If an account exists in the forest with the same User Principal Name, adapter will fail the user add request.

Case 2: User Principal Name is not supplied in the user add request.

When User Principal Name is not provided in user add request, adapter will generate the value for this attribute. (Please refer "Chapter 3. Active Directory Adapter user account management tasks->Adding user accounts->User principal name of a user account section" for more detail). Adapter then uses this generated User Principal Name to perform search in the forest. If adapter finds a user account with this generated User Principal Name it then appends a number, starting from 1, to the generated value to get a new User Principal Name.

Example,

Let's consider that adapter has generated the User Principal Name as TestUser@MyDomain.com. If it is found to be used by an existing user account, adapter will then append the number 1 to generate the new value as TestUser1@MyDomain.com.

Now adapter will perform a search using this new value. If even the User Principal Name TestUser1@MyDomain.com is found to be used, again a new value is generated by appending number 2 as TestUser2@MyDomain.com. If TestUser2@MyDomain.com is also already in use, adapter will fail the user add request.

Note:

1. The User Principal Name's search operation is costly in terms of adapter performance.
2. Due to replication delay adapter may not find a user with the current User Principal Name and will add the user account.
3. If there are two simultaneously running add request with the same User Principal Name, adapter may not find a user with the User Principal Name and both the user accounts will get added successfully.

It is recommended that you should have policy to generate unique User Principal Name on IBM Tivoli Identity Manager Server and should not rely on adapter to generate unique name.

Improve primary group lookup using cache

The reconciliation of primary group is costly operation and so a registry key "ReconPrimaryGroup" is used by adapter to improve reconciliation performance by setting this key to FALSE. This version of Windows Active Directory Adapter is improved to minimize primary group lookup searches using a local cache. If a set of users have the same primary group, then the lookup for that primary group will be done only once and not for each user account during a reconciliation operation.

Note: The primary group is cached for a particular reconciliation operation. If in your setup each user or most of users has different primary group then the benefit of this enhancements are nullified. With this version the default value of '**ReconPrimaryGroup**' is changed to **FALSE**'.

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 both through the use of pre-Exec and post-Exec scripting and schema extensions using the extschema.txt file.

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 64-bit
- Windows 2008 64-bit

Managed Resource:

- Windows 2003 Enterprise Edition with Active Directory
Exchange 2007 (optional)

- Windows 2008 Enterprise Edition with Active Directory
Exchange 2007 (optional)

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

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.

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