

Release Notes



IBM® Tivoli® Identity Manager Active Directory (WinAD) Adapter

Version 4.6.24

Tenth Edition (April 25, 2009)

This edition applies to version 4.6 of this Adapter and to all subsequent releases and modifications until otherwise indicated in new editions.

IBM, Tivoli, and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Windows is a trademark of Microsoft® Corporation in the United States, other countries, or both.

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

Other company, product, and service names may be the trademarks or service marks of others. U.S. Government Users Restricted Rights – Use, duplication, or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

© Copyright International Business Machines Corporation 2004, 2009. All rights reserved.

US Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Preface	3
Adapter Features and Purpose	3
Contents of this Release	4
Adapter Version	4
New Features	4
Closed Issues	7
Known Issues	14
Installation and Configuration Notes	17
Corrections to Installation Guide	17
Configuration Notes	17
General Configuration Notes	17
Using the new WinAD Agent Features	20
New Adapter Options (Registry Keys).....	20
1. useSSL	20
2. useDefaultDC	20
3. useGroupCN	21
4. delUNCHomeDirOnDeprovision.....	23
5. delRoamingProfileOnDeprovision	24
6. MailboxPermissionsEnabled	24
7. Bypass Microsoft API for processing X500 Proxy addresses:	25
8. Enable/disable Add/Mod operation for Mailbox permissions:	25
9. Enable/disable recon for mailbox permissions:	26
10. Enable/disable "UseThreadPooling":	26
New Features in this version of the Adapter	27
1. Mailbox Move	27
2. Use new Win2003 ADSI API for managing WTS attributes.....	27
3. Win AD Agent handle Add and Delete operations for erGroup attribute	27
4. Running Mixed Versions of Active Directory and Exchange.....	28
5. AbortReconOnFailure	28
6. Custom Proxy Addresses.....	28
7. Dial-In Options.....	29
8. lastLogonTimeStamp attribute	30
Supported Configurations	31
Installation Platform	31
Deployment Configurations	32
Notices	40
Trademarks.....	41

Preface

Welcome to the IBM Tivoli Identity Manager Windows Active Directory 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 Windows Active Directory Adapter Installation and Configuration Guide

Adapter Features and Purpose

The Windows Active Directory (WinAD) Adapter is designed to create and manage Active Directory accounts within a Windows 2000 or Windows2003 domain. The adapter can optionally manage Exchange 2000 or Exchange 2003 mailboxes within the same domain. This Adapter does not create or manage local system accounts. Please use the Windows Local Account Adapter for this purpose.

IBM recommends the installation of this Adapter on a Windows 2000, Windows 2003 or XP workstation within the domain being managed. Typically, one adapter is installed per domain, but the WinAD Adapter may be configured to support both sub-domains and multiple domains through the Base Point Feature on the WinAD Service Form. The optimum deployment configuration is based, in part, on the topology of your windows 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 Policy, Organization & Administration Guide for a discussion of these topics.

The WinAD Adapter is a powerful tool that requires Administrator Level authority. The Adapter operates much like a human system administrator, creating Active Directory accounts, Exchange mailboxes, 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 local or domain level administrative permissions.

Contents of this Release

Adapter Version

Component	Version
Release Date	April 25, 2009
Adapter Version	4.6.24 (build 4.6.1026)
Comm. Libraries	ADK v4.803
Documentation	Windows Active Directory Installation and Configuration Guide v4.6.0 SC32-1376-10

New Features

Enhancement # (FITS)	Description
	Items included in current release
	None
	Items included in 4.6.23 release
MR0427076459	Add support for lastLogonTimeStamp attribute. See additional information in the "New Features of this Adapter" section.
	Items included in 4.6.22 release
MR1118053029	WinAD: Enhance the adapter to handle all the options of the "Remote Access Permission" property NOTE: If you have any business logic (e.g. Provisioning Policy Parameter) around attribute "erADAllowDialin" then you must modify it to use "erADExDialin". See additional Notes under "Dial-In Options" in the New Features section of this document.
	Items included in 4.6.20 release
MR0206075137	Win PW Sync: Reverse Password Sync Util enhancement request. Support for 64 bit OS and hardware
MR0209071753	Win PW Sync: Wants Reverse Password synch supported on 2003 64bit machine
MR050806335	Win PW Sync: allow the PwdSync agent to enforce the password change to Local Windows Policy if the request fails. This option automatically changes Verify setting to "off" on a failure to contact TIM.

Enhancement # (FITS)	Description
	Items included in release 4.6.18
MR0713074158	Enhance WinAD proxy support to allow entry of custom email types.
	Items included in release 4.6.11
MR0509064953	Enhance performance of Single user lookup. Do not create group map (which optimizes full Recon).
MR0517066713	Revise AD Adapter to minimize Windows AD replication delays. Results in "failure to set share permission" in some environments.
	Items included in release 4.6.5
	Please see "Using the new WinAD Agent Features" (below) for information on how to use the enhancements.
MR0921053414	WinAD: Add support for additional combinations of Windows and Exchange versions to simplify Windows and Exchange upgrades. This agent now supports Windows AD 2003 with Exchange 2000. NOTE: Important restrictions apply. Please see "Using the new WinAD Agent Features" (below) for information on how to use the enhancement.
N/A	Allow option to bypass Microsoft API for processing X500 Proxy address. This adapter options is a work-around for Microsoft Bug described in Microsoft Case ID SRZ050912001439 CAUTION: IBM does not recommend the use of this option. Please see additional warnings in "Using the new WinAD Agent Features" (below).
N/A	Allow the option to enable/disable Add/Modify operations for mailbox permissions and allow the option to enable/disable Recon of mailbox permissions.
	Items included in release 4.6.4
MR0921053414	WinAD: Add support for additional combinations of Windows and Exchange versions to simplify Windows and Exchange upgrades. This agent now supports Windows AD 2003 with Exchange 2000.

Enhancement # (FITS)	Description
	Items included in release 4.6.3
	Please see "Using the new WinAD Adapter Features" (below) for information on how to use the enhancements.
MR1111044841	Use the ADS_USE_SSL option when connecting to AD.
MR041505734 MR0607053035	Allow option to use Hostname in Basepoint, but if "down", reconnect to the default AD controller.
MR042905280 MR0314051848	Use group CN instead of GUID.
MR0420052456	Delete home directory (and files) on deprovision
MR042005253	Delete Profile path (and files) on deprovision
MR0428055048	Support Mailbox Move function.
MR0429056225	Use new Win2003 ADSI API for creating WTS
MR0804053247	Agent to handle Add and Delete operations for group
	Items included in 4.6.0 release
	Updated Adapter for compatibility with ITIM 4.6.

Closed Issues

DevTrack	APAR#	PMR# / Description
		Items closed in current version
		This version of the adapter requires an updated profile. Please see 'Configuration Notes' before installing this adapter.
	IZ42815	67170,650,706 WinAD Adapter installer issue if the path contains a space.
	IZ44751	17064,642,760 ITIM WinAD 64 Bit Crash. (applies to 32-bit also)
	N/A	28577,227,000 WinAD Adapter crashes randomly (associated with IZ47418)
	N/A	N/A Internal ADK related fixes. <ul style="list-style-type: none"> - ADK crash in SSL_read_error while reading error message after a handshake failure. - CMVC #35017 - ADK Crash in recon when user EntryDN contains 'pass'/'pwd'. - CMVC #35175 - Adapter returns unreadable error msg for multivalued attribute. -
		Items closed in 4.6.22 version
N/A	IZ24107	37721,550,000 AD Adapter error while creating home directories.
32557	N/A	N/A AD Agent sees WTS drive letter instead of WTS home directory in "Local Path" on AD.
32579	N/A	N/A WinAD wrongly set Dialin when "Fixed callback number" is selected.

DevTrack	APAR#	PMR# / Description
		Items closed in 4.6.22 version
N/A	IZ10903	<p>WinAD adapter memory leak.</p> <p>There is an issue with the Microsoft CDOEXM library used by Active Directory Agent to perform Exchange tasks. A ticket is also opened with Microsoft, Case ID "SRZ080104000181", for the same.</p> <p>Solution: Agent is redesigned as described in Microsoft Case ID. A new registry key "UseThreadPooling" is introduced. By default this key is set to "FALSE" so that existing customers are not affected.</p> <p>When UseThreadPooling is set to TRUE Thread Pooling is enabled, with all the threads initialized at the start of Agent Service and uninitialized when the Agent service stops. When UseThreadPooling is set to FALSE Thread Pooling is disabled. In this scenario threads will be created and destroyed on per request.</p> <p>Note: If you are experiencing high memory usage then set this key to "TRUE".</p> <p>See additional Notes under "Thread Pooling Options" in the New Registry Keys section of this document.</p>
N/A	IZ13159	<p>Enhancement to support the third dial-in option "Control access through Remote Access Policy"</p> <p>NOTE: If you have any business logic (e.g. Provisioning Policy Parameter) around attribute "erADAllowDialin" then you must modify it to use "erADExDialin".</p> <p>See additional Notes under "Dial-In Options" in the New Features section of this document.</p>

DevTrack	APAR#	PMR# / Description
		Items closed in 4.6.21 version
	IZ14154	38318,L6Q,000 Incorrect response on group modification. Transaction status not properly set if the successful action was to set one value of a multi-valued attribute.
	IZ14468	23949,292,848 The street attribute is not set properly on the resource. The XML parser in ADK removes \r from newline.
31875		(internal) Adapter reports success for mailbox perm. attribute but AD not updated.
		Items closed in 4.6.20 version
N/A	N/A	N/A Updated Release Notes for PW Synch Plug-In
		Items closed in 4.6.19 version
N/A	IZ09072	20243,999,760 TIM Express is unable to set some AD Account password attributes.
		Items closed in 4.6.18 version
		None
		Items closed in 4.6.17 version
N/A	IZ00891	68950,L6Q,000 AD Agent recon gets the following error while processing the AD Containers: Container search failed. Error code: 0x000000ea - Calling GetNextRow can potentially return more results. Provider: LDAP Provider. May occur if AD is under load.
		Items closed in 4.6.16 version
N/A	IY98259	70424,227,000 AD Agent does not consistently send password on account restore. Status to ITIM server does not show failure if Adapter option is set to unlock the account on a password reset.
N/A	IY97544	42563,057,649 Memory leak in AD Agent during recon

DevTrack	APAR#	PMR# / Description
		Items closed in 4.6.15 version
N/A	IY93989	61936,004,000 Attributes with only special characters cause Adapter to crash.
N/A	IY96264	65275,422,000 Unable to remove Home Directory share during account modify.
		Items closed in 4.6.14 version
N/A	IY91044	31753,035,724 WinAD adapter cannot manage the eradnochange password attribute on non-English systems.
N/A	IY91565	PMR 92121,L6Q,000 erUid truncated to 20 characters when creating AD account. WinAD adapter changed to return an error if Win Account Name is too long (Windows allows a max of 20 characters)
		Items closed in 4.6.13 version
S17553	IY89396	86618,L6Q,000 Need to reduce overhead in AD adapter with exschema.txt file during startup. Using the schema extension capability may result in agent startup times longer than 30 seconds, causing a Windows service to timeout on startup.
S17534	IY88919	94913,292,848 ADSI Error: 0x80072024 not handled properly. See new Configuration Option – AbortReconOnFailure.
S17341	IY84890	55259,379,000 and 59749,227,000 Windows AD adapter crash when trying to change value of existing mailstore attribute with Exchange 2003sp2. See “Known Restrictions” section (below) for additional details on this topic.
		Items closed in 4.6.12 version
S17494	IY84890	55259,379,000 Exchange Mailbox Permissions Function Always Gets Called
S17437	IY86177	09611,999,760 When AD agent is installed on Windows 2003, timeout values for terminal server are incorrectly set in minutes.

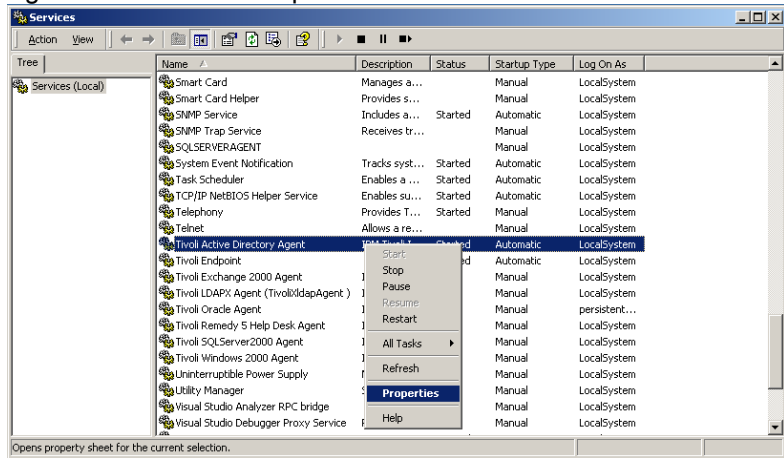
DevTrack	APAR#	PMR# / Description
		Items closed in 4.6.11 version
C15438	IY86118	06908,379,000 Active Directory provisioning not working as expected when Exchange Mailbox Alias value is removed and then added back.
S17424	IY85876	83403,057,649 AD Adapter Hang.
		Items closed in 4.6.10 version
C15438	N/A	N/A The default value of Thread Priority Level is wrong.
S17192	IY81588	05204,249,649 Event notification list can not exceed 4096 chars. NOTE: a full Recon must be run before enabling Event Notification.
S17173	IY81175	06908,379,000 Removal of Alias for user in AD yields error the root element is required in a well-form document.
S17292	IY83920	94936,999,760 "Some attributes were not modified" error occurred when modifying AD primary group, but the attribute was changed as expected.
S17222	IY81997	69864,49R,000 AD Agent event notification does not process AD Container additions properly. Get LDAP 34 error, invalid DN syntax.
S17132	IY80075	67941,379,000 AD Event notification crashes.
S17187	IY81465	12754,379,000 AD agent MailboxPermissionEnabled warnings.
		Items closed in 4.6.9 version
C15673	N/A	N/A Removed Logon Date/Time grid from the default Profile. NOTE: Profile must be reinstalled.
N/A	N/A	N/A Updated Installation and Configuration Guide packaged with this release.

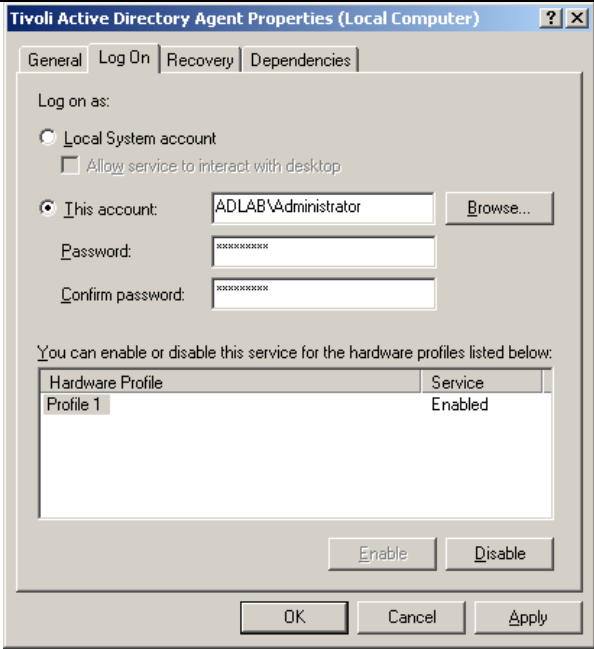
DevTrack	APAR#	PMR# / Description
		Items closed in 4.6.8 version
S17161	IY79827	70193,227,000 Win AD agent may run out of memory waiting for the ITIM server to read Recon results if connection to the ITIM server is lost.
C13005	N/A	N/A WinAD search for "Forwarding address" attribute returns no results. NOTE: This fix requires the WinAD Agent Profile to be reinstalled.
		Items closed in 4.6.7 version
S17110	IY79670	49177,227,000 ADagent always attempts to set MailboxPermissions on modify.
S17095	IY79289	67135,379,000 AdAgent MailboxPersmissionsEnabled registry read fails (ADK fix. ADK 4.67)
		Items closed in 4.6.6 version
C11976	N/A	N/A Recon reports success despite failure.
C11544	N/A	N/A Compatibility with WAS 6.0. Event Notification not working. ADK updated to version 4.67.
		Items closed in 4.6.5 version
S17047	IY78197	14893,035,649 AD Account Password does not use password widget on default Service form. NOTE: Requires reinstallation of the WinAD profile.
S17057	IY78527	43546,379,000 Transaction to add a new WinAD account may fail under load. Thread deadlock in SetNoChangePassword function.
C11976	N/A	N/A WinAD service form owners & prerequisite fields not present on default Service Form. NOTE: Requires reinstallation of the WinAD profile.

DevTrack	APAR#	PMR# / Description
		Items closed in 4.6.4 version
S16796	IY75243	10059,379,000 Incorrect newline translation with multi-line attributes and AD Agent.
S16953	IY76848	26633,227,000 Fetching Exchange mailbox permissions take long time with remote Exchange locations. NOTE: A registry key MailboxPermissionsEnabled is introduced. If this key is set to TRUE or key does not exists, agent will handle mailbox permissions. If this key is set to FALSE, agent will not handle mailbox permissions. By default this key is set to TRUE.
		Items closed in 4.6.3 version
N/A	N/A	N/A Adapter repackaged with version 4.65 ITIM communication libraries (ADK).
N/A	N/A	N/A Memory leak in Recon process. COM object not freed properly.
		Items closed in 4.6.2 version
S16745	IY74884	20945,49R,000 If an account is added, but an exchange account is not created at the same time, the request will complete, but with warnings. NOTE: updated Agent Profile must be installed.
		Items closed in Release 4.6.1
S16708	IY74558	01586,379,000 Active Directory Agent terminates when "replace" DAML message contains the "erPassword" attribute with a null value. NOTE: if a Null password value is sent to the adapter, it will now attempt to remove the existing password from the account. This transaction will fail unless AD password policies allow null passwords.

Known Issues

DevTrack	APAR#	PMR# / Description
N/A	N/A	N/A User ID and container field cannot contain the character "#". Gives "User not created" error on Add transaction. 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.
		IMPORTANT NOTE: The Windows AD agent is designed to automatically detect and bind to Exchange if present in your domain. If Exchange is not present the following Log File message will appear. This error can be safely ignored. DBG: <date time> Enumerating Exchange servers... DBG: <date time> Unable to bind to CN=Microsoft Exchange...
		IMPORTANT NOTE: The Windows AD agent does not use an xforms.xml file. Errors in the Agent Log concerning xforms may be safely ignored. Error message is: "Unable to load XML transformation buffer from..."
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 <i>CoInitialize</i> and upon operation completion calls <i>CoUninitialize</i> 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.

DevTrack	APAR#	PMR# / Description
S17341	IY84890	<p>55259,379,000 and 59749,227,000</p> <p>Windows AD adapter crash when trying to change value of existing mailstore attribute with Exchange 2003sp2. This condition may occur if an "Administration User Account" is specified on the Service Form.</p> <p>The recommendation is to run the Windows Service using this Account instead of specifying it on the Service form.</p> <p>The issue results from a restriction in Active Directory APIs. The details and case number are listed below.</p> <p>If "Administration User Account" and "Administration User Password" is given on AD service form on ITIM side and AD agent is running either as service or in console mode, CreateMailbox API of IMailboxStore fails to create mailbox. If we leave administrator username and password field blank on Ad service form on ITIM side and run "Tivoli Active Directory Agent" windows service under domain administrator account by configuring windows service "Log on as:" property then mailbox gets created successfully. For more information refer Microsoft Case ID SRZ060616001384.</p> <p>This affects the Deployment Configurations scenario 8 (Page: 26, Scenario 8: Adapter on Adapter Server in Multi-Domain Active Directory). This scenario will be supported provided both domain "Doamin1" and "Domain2" has common domain administrator.</p> <p>Steps to configure "Tivoli Active Directory Agent" windows service:</p> <ol style="list-style-type: none"> 1. Open the windows Services panel. Select "Tivoli Active Directory Agent" and click on "Properties".  <ol style="list-style-type: none"> 2. Click on "Log On" tab. Select "This account" and enter domain administrator username and password. Click on "OK" to close the properties page.

		
--	--	------------------------------------------------------------------------------------

Installation and Configuration Notes

See the IBM Tivoli Identity Manager Windows Active Directory Adapter Installation Guide for detailed instructions.

Corrections to Installation Guide

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

None.

Configuration Notes

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

Correction to the Active Directory Adapter Installation and Configuration Guide

Appendix B, Adapter attributes, table 14 lists attribute erPasswordExpiresOn as one of the supported attributes by the adapter. This information is incorrect. This is an error in the guide. The adapter does not support such an attribute.

General Configuration Notes

Profile Updated in Version 4.6.23 on this Adapter

The following applies only to customers who have installed the profile shipped with Adapter build 4.6.1024. Only 4.6.1024 is affected. If you are upgrading from earlier profile versions you are not affected.

If you have the adapter profile supplied with Adapter-WinAD-4.6.22 version (adapter build 4.6.1024) installed on your system, 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.

Multi-Instance Settings

Agent multi-instance settings in the agentCfg tool is not a supported feature. The agent uses the BasePoint feature to manage multiple sub-domains.

Adding a Primary Group

To add a primary group to a user, the user must be a member of the group.

Mailbox Configuration

- The Mailstore attribute cannot be set without an Alias.
- The Target Address attribute cannot be set without an Alias.
- The Mailstore and Target Address attributes are mutually exclusive.
- To delete a Mailbox, delete the Alias attribute. Submit a reconciliation request to clear unnecessary values from the account form and to verify that the mailbox has been removed.

Proxy Address Configuration

- A primary proxy address for each type must be added before additional proxy addresses of the same type can be added. Primary proxy addresses are identified by capital letters. For example, 'SMTP:user1@ibm.com' is a primary address and 'smtp:user2@ibm.com' is a secondary proxy address.
- The primary SMTP address cannot be deleted.
- Adding proxy address(es) when creating a mailstore for an account may fail due to timing issues (Exchange propagation delays) . Perform a reconciliation to verify that the proxy address(es) were added. If they were not added to the account, submit a modify request to add the proxy addresses.

The Win AD Agent requires that the Primary SMTP Address be set before setting the X.400 email address in proxy addresses field.

Directory Creation

Directories can only be created one level deep. For example "c:\directory1" can be created, but "c:\directory1\directory2" cannot be created.

Directory Deletion

Directories can only be deleted if they are empty. If the directory is not empty, the directory attributes will be cleared but the directory will still remain in tact.

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.

ReconPrimaryGroup Setting

A new registry key ReconPrimaryGroup is used to determine if the agent will recon the primary group attribute.

- a. If its value is true or the key does not exist in the registry, the user will thus be able to see the primary group in both the Group field and Primary Group field in ITIM.
- b. If its value is false, the primary group will not be seen in Group field and also not in Primary Group field in ITIM.

WTS Recon Default

The Recon default for WTS attributes has been changed to "OFF".

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. I suppose the AD Agent is running on AD server itself. Moving the AD Agent onto a different machine would take off some load from DS.

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/>. The two minute time limit as well as maximum page size can be configured.

Using the new WinAD Agent Features

New Adapter Options (Registry Keys)

The following new registry key settings are now available

1. useSSL

This registry setting 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).

2. useDefaultDC

This 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.

IMPORTANT NOTE: 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.

3. useGroupCN

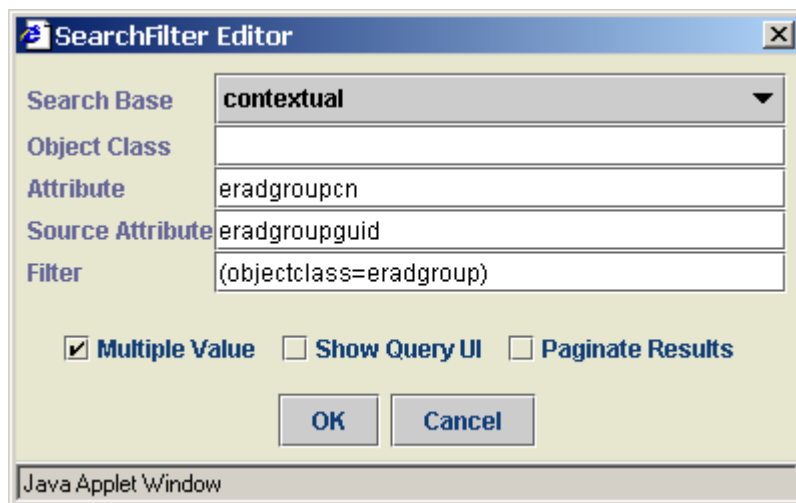
This registry setting allows switching between group CN and group GUID. If TRUE, agent will use group CN to process groups. If FALSE, agent will use group GUID to process groups.

By default this key is set to FALSE.

Following ITIM side changes are required to use this feature.

A. To use Group CN:

1. Using agentCfg set useGroupCN to TRUE.
2. Logon to the Tivoli Identity Manager Server, using an account that has the authority to perform administrative tasks.
3. Select Configuration from the Main Menu Navigation Bar.
4. Click on USER INTERFACE CUSTOMIZATION tab.
5. Navigate through the Account tree and select ADAccount
6. Click on tab.ad.account tab of ADAccount form.
7. Double click the \$ergroup attribute. It will bring following screen.



8. Change Source Attribute (in the above figure) to **eradgroupcn** and click OK button.
9. Double click the \$eradprimarygroup attribute. The following screen is shown.

SearchFilter Editor

Search Base: **contextual**

Object Class:

Attribute: **eradgroupcn**

Source Attribute: **eradprimarygrptkn**

Filter: **(objectclass=eradgroup)**

☐ Multiple Value ☐ Show Query UI ☐ Paginate Results

OK **Cancel**

Java Applet Window

10. Change Source Attribute (in the above figure) to **eradgroupcn** and click OK button
11. Run full reconciliation. This will ensure that agent is sending group CN instead of group GUID and will be stored in ITIM LDAP.

After switch, in next Add / Mod operations ITIM will send group CN to agent for user group memberships and primary group.

B. To use Group GUID:

1. Using agentCfg set useGroupCN to FALSE.
2. Logon to the Tivoli Identity Manager Server, using an account that has the authority to perform administrative tasks.
3. Select Configuration from the Main Menu Navigation Bar.
4. Click on USER INTERFACE CUSTOMIZATION tab.
5. Navigate through the Account tree and select ADAccount
6. Click on tab.ad.account tab of ADAccount form.
7. Double click the \$ergroup attribute. It will bring following screen.

SearchFilter Editor

Search Base: **contextual**

Object Class:

Attribute: **eradgroupcn**

Source Attribute: **eradgroupcn**

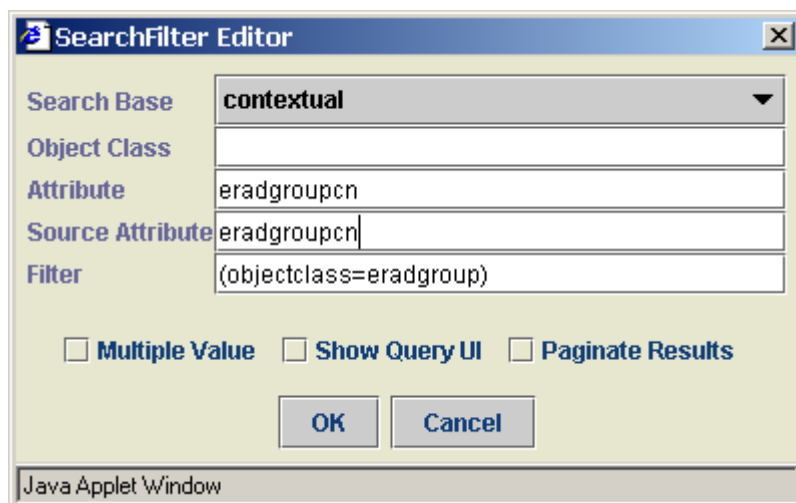
Filter: **(objectclass=eradgroup)**

☒ Multiple Value ☐ Show Query UI ☐ Paginate Results

OK **Cancel**

Java Applet Window

8. Change Source Attribute (in the above figure) to **eradgroupguid** and click OK button.
9. Double click the \$eradprimarygroup attribute. The following screen is shown.



10. Change Source Attribute (in the above figure) to **eradprimarygrptkn** and click OK button
11. Run full reconciliation. This will ensure that agent is sending group GUID instead of group CN and will be stored in ITIM LDAP.

After switch, in next Add / Mod operations ITIM will send group GUID to agent for user group memberships. For primary group ITIM will send primary group token to agent.

4. delUNCHomeDirOnDeprovision

This registry setting is to enable UNC Home directory deletion when user is de-provisioned. Agent handle only UNC home directory path (e.g. [\\servername\sharename\<home directory>](#) and not local path (e.g. "c:\<directory>").

If TRUE, agent will delete user home directory (subdirectories and files) after successfully deleting the user from AD. If this key is not present or FALSE, agent will not delete user home directory.

By default this key is set to FALSE.

This registry setting also affects WTS home directory and will be used in conjunction with **wtsEnabled** registry setting. If wtsEnabled is set to TRUE then WTS home directory and files will be deleted.

Following table illustrate the behavior of agent depending on registry key settings.

delUNCHomeDirOnDeprovision	WtsEnabled	User Home Dir	WTS Home Dir	Comments
TRUE	TRUE	Deleted	Deleted	No warning or error as such will be sent to ITIM if directory delete fails (errors will be logged in log file). If user deletion from AD fails then operation will be failed.
TRUE	FALSE	Deleted	Not deleted	
FALSE	TRUE	Not deleted	Not deleted	
FALSE	FALSE	Not deleted	Not deleted	

5. delRoamingProfileOnDeprovision

This registry setting is to enable user profile directory deletion when user is de-provisioned. The agent will manage roaming user profiles only as the profile and profile files are stored on a share. This will be the UNC path (e.g. [\\servername\sharename\<profile directory>](#) and not local profile.

If TRUE, agent will delete user profile directory (subdirectories and files) after successfully deleting the user from AD. If this key is not present or FALSE, agent will not delete user home directory.

By default this key is set to FALSE.

Agent must be run under account, which has permission to delete user profile directories.

This registry setting also affects WTS profile directory and will be used in conjunction with **wtsEnabled** registry setting. If wtsEnabled is set to TRUE then WTS user profile directory and files will be deleted.

Following table illustrate the behavior of agent depending on registry key settings.

delRoamingProfileOnDeprovision	WtsEnabled	User profile directory	WTS profile directory	Comments
TRUE	TRUE	Deleted	Deleted	No warning or error as such will be sent to ITIM if profile delete fails (errors will be logged in log file). If user deletion from AD fails then operation will be failed.
TRUE	FALSE	Deleted	Not deleted	
FALSE	TRUE	Not deleted	Not deleted	
FALSE	FALSE	Not deleted	Not deleted	

6. MailboxPermissionsEnabled

Retrieving mailbox permissions on remote Exchange servers may be very slow, potentially causing the ITIM transaction to time out. A new registry key MailboxPermissionsEnabled is introduced to optionally bypass the mailbox permission processing.

If this key is set to TRUE or key does not exists, agent will set and retrieve mailbox permissions. If this key is set to FALSE, agent will not handle mailbox permissions. By default this key is set to TRUE.

7. Bypass Microsoft API for processing X500 Proxy addresses:

This enhancement allows the agent to bypass Microsoft API for proxy addresses. A registry key OverrideX500Addresses is introduced. If this key is set to TRUE, agent bypasses Microsoft proxy address API to set proxy addresses. X500 address is set as standard LDAP string attribute (using PutEx method).

If this key is not present or set to FALSE, agent will use Microsoft proxy address API (put_proxyAddresses). This key is set to FALSE by default. No ITIM server-side changes are required to use this enhancement.

NOTE: Microsoft Proxy address API does a format checking and duplicates checking on the provided list of proxy addresses. Even if one address does not comply, the API returns failure.

There is issue with X500 proxy address, as this is not supported by exchange 2000 and 2003 (exchange 5.5 supports but when migrated to exchange 2000 it's no longer available).

By setting OverrideX500Addresses to TRUE, agent will filter the X500 address and will treat it as standard LDAP string attribute. Agent does not do any format checking and duplicate checking as done by the Microsoft API. For rest of the proxy addresses agent will use Microsoft API.

It's the responsibility of end user to specify the X500 address in correct format. Incorrect X500 address may affect other applications which are using X500 addresses.

WARNING: use of this option is not recommended by IBM.

The configuration option has been implemented at the advice of Microsoft to work-around a known bug in the Windows 2000/2003 Operating system (see case # SRX050919605805).

Use of this option bypasses the Microsoft APIs to set and retrieve SMTP addresses. It is the responsibility of the customer to ensure that SMTP addresses comply with all Microsoft Active Directory restrictions. These restrictions include, but are not limited to:

- Format of SMTP addresses
- Legal character sets
- Duplicate SMTP addresses

FAILURE TO ADHERE TO PROPER DATA VALIDATION MAY RESULT IN DATA CORRUPTION OR DATA LOSS WITHIN ACTIVE DIRECTORY. PLEASE CONSULT MICROSOFT FOR A COMPLETE LIST OF THESE DATA VALIDATION RULES.

8. Enable/disable Add/Mod operation for Mailbox permissions:

This enhancement allows agent to enable or disable adding or modifying mailbox permissions. A registry key MailboxPermissionsEnabled is introduced. If this key is set to TRUE, agent will process mailbox permission attributes in Add/Mod operation.

If this key is not present or set to FALSE, agent will not process mailbox permissions attributes. This key is set to FALSE by default. No ITIM server-side changes are required to use this enhancement.

9. Enable/disable recon for mailbox permissions:

This enhancement allows agent to enable or disable returning mailbox permissions in recon. A registry key ReconMailboxPermissions is introduced. If this key is set to TRUE, agent will recon mailbox permission attributes.

If this key is not present or set to FALSE, agent will not recon mailbox permissions attributes. This key is set to FALSE by default. No ITIM server-side changes are required to use this enhancement.

10. Enable/disable "UseThreadPooling":

There is an issue In the Microsoft CDOEXM library used by Active Directory Agent to perform Exchange tasks. A ticket is also opened with Microsoft, Case ID "SRZ080104000181", for the same.

Agent is redesigned as described in Microsoft Case ID. A new registry key "UseThreadPooling" is introduced. By default this key is set to "FALSE" so that existing customers are not affected. When UseThreadPooling is set to TRUE Thread Pooling is enabled, with all the threads initialized at the start of Agent Service and uninitialized when the Agent service stops. When UseThreadPooling is set to FALSE Thread Pooling is disabled. In this scenario threads will be created and destroyed on per request.

Note: If you are experiencing high memory usage then set this key to "TRUE".

New Features in this version of the Adapter

1. Mailbox Move

Agent now supports “Move mailbox” functionality between different mail store on same exchange server or different exchange servers in the same domain.

2. 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.

3. Win AD Agent handle Add and Delete operations for erGroup attribute

AD Agent honors only replace operation from ITIM. This is based on the ITIM default behavior where ITIM sends operation as replace for modification of group.

Agent now supports Add and Delete operation for erGroup attribute for Modify request.

On ITIM side profile changes are required in ADprofile to send group operation as add, delete for modify request. See the steps below

- ☐ Add the following line in xforms.xml file.

```
<EnRoleAttribute Name="erGroup" RemoteName="erGroup" ConvertReplaceToAddDelete="true"/>
```

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

4. Running Mixed Versions of Active Directory and Exchange

The agent is certified to run in Windows 2003 Active Directory and Exchange 2000 Exchange server environment. Windows 2003 Active Directory and Exchange 2000 on same server is not a valid configuration. These must be installed on separate machines.

The following limitations apply to this mixed mode environment:

- 1) A domain controller must be specified as a part of base point to create mailbox on the Member server.
- 2) Mailbox move is not supported in a mixed mode environment. Move mailbox operation will fail when an attempt is made to move a mailbox from or to a mailstore on the member server.
 - a. Move mailbox from a Mailstore on Member server to a Mailstore on Primary DC **fails**.
 - b. Move mailbox from a Mailstore on Member server to another Mailstore on Member server **fails**.
 - c. Move mailbox from a Mailstore on Primary DC to another Mailstore on Primary DC **succeeds**.

5. AbortReconOnFailure

Agent performs a search for group information and user account information and then it binds to respective object to fetch more information. It is possible that the adapter may receive an ADSI API error 0x80072024 (The administrative limit for this request was exceeded.). This switch controls the behavior of the adapter when this condition is encountered.

If this key is set to TRUE, the adapter will abort the recon on ADSI API error 0x80072024 and will return failure to ITIM.

If this key is set to FALSE, agent will ignore error and will continue to fetch next group and/or user information. The group or account for which the error occurred will not be returned to ITIM. In such case information about group and/or account will be removed from ITIM. This is the default behavior and the behavior as it existed in prior versions of the adapter.

6. Custom Proxy Addresses

Usage: Agent has been enhanced to support proxy addresses of any custom type. No configuration is required to use this feature. The adapter now allows the entry of any proxy type and value in the Proxy Address attribute.

Technical Notes: If the proxy type is one of the known Microsoft types, the ADSI API calls will be made to set the value. If it is not a known type, the proxy type and value will be set directly to AD and treated as a string attribute.

The previous versions of the WinAD adapter did not support eradeproxyaddresses other than SMTP and X400 types. The old configuration setting "OverrideX500Addresses=TRUE" only worked for X500 addresses.

Beginning with this version of the adapter, the registry key "OverrideX500Addresses" is deprecated. The new registry key "SupportedProxyEmailTypes" is introduced. This new key will hold comma separated list of supported proxy email types. The default value for this key is SMTP;,X400: This list

represents the Microsoft supported (i.e. standard) Proxy types allowed by the API. (This is NOT a list of the proxy types the ITIM customer will use)

Here supported proxy email type means supported by Microsoft API put_ProxyAddresses method. If you want any other proxy email type to be treated as standard supported type then append the type including separator(:) to existing value.

For example, if you want SIP to be treated as supported type then the SupportedProxyEmailTypes registry key value will be SMTP:,X400:,SIP:

For the proxy email types "other than" specified in the registry key, agent will filter those addresses and will treat as standard LDAP string values. The adapter will not do any error checking; duplicate checking as done by the Microsoft API.

Warning: Microsoft API does a format checking and duplicates checking on the provided list of proxy addresses. Even if one address does not comply, the API returns total failure. There is issue with proxy addresses apart from SMTP and X400, as this is not supported by exchange 2000 and 2003

It is the sole responsibility of end user to specify the correct proxy email addresses. Incorrect proxy email address may affect other applications which are using custom proxy email addresses.

7. Dial-In Options

A new attribute "erADExDialin" is added to support this enhancement. A new String attribute "erADExDialin" is added in erADAccount object class.

Attribute "erADExDialin" is added to the Active Directory accounts form (erADAccount.xml). The account form now has a combo box instead of a checkbox representing one the three values for dial-in.

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

Attribute "erADAllowDailin" is deprecated and will not be processed by AD Agent

Attribute "erADAllowDailin" is removed from the accounts from.

Note:

- 1) If you have any business logic around attribute "erADAllowDialin" (e.g. a Provisioning Policy Parameter) then you must modify it to use "erADExDialin".
- 2) 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". If previously dial-in was set to "Allow Access" after the above failed request dial-in will be set as "Deny Access".

8. 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.

To support this enhancement 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.

Supported Configurations

Installation Platform

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

Adapter Installation Platform:

- Windows 2000 Server or Workstation
- Windows XP Workstation
- Windows 2003 Server
- Windows 2003 R2 Server

Managed Resource:

- Windows 2000 Server with Active Directory
- Exchange 2000 with Service Pack 2, or Service Pack 1 and the post-Service Pack 1 Exchange 2000 hotfix (optional)
- or --
- Windows 2003 Enterprise Edition with Active Directory
- Exchange 2003 (optional)
- or --
- Windows 2008 Enterprise Edition with Active Directory (See Note below)
- Exchange 2003 (optional)

IBM Tivoli Identity Manager:

- ITIM 4.6.0 or later

IMPORTANT NOTE:

- This Adapter supports the following configurations:
- Windows 2000 with optional Exchange 2000 (Adapter installed on a Win 2000 server)
- Windows 2003 with optional Exchange 2000 (Adapter installed on a Win 2003 server)
- Windows 2003 with optional Exchange 2003 (Adapter installed on a Win 2003 server)

No other configurations are supported.

NOTE: Microsoft recommends using a version of the Exchange Admin Tools that match the version of Exchange.

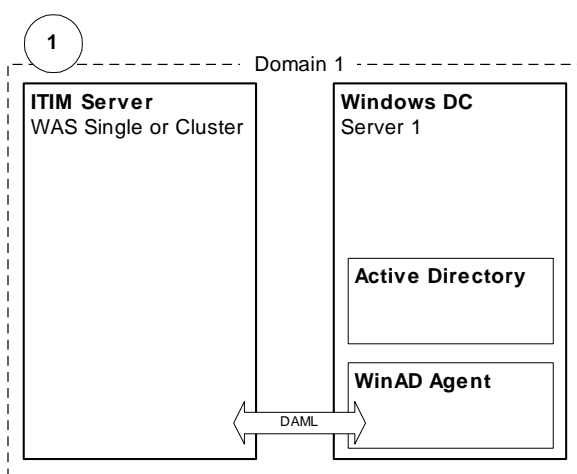
NOTE: Windows AD 2008 can be managed by the adapter, but the adapter must be installed on a 2003 system.

Deployment Configurations

The following section includes details of several supported WinAD Adapter deployment configurations. If your intended deployment is not explicitly listed as “supported,” please contact IBM Identity Manager Support to confirm your configuration prior to deployment.

Windows Active Directory Adapter

Deployment Configuratons for Windows and Exchange 2000 / 2003

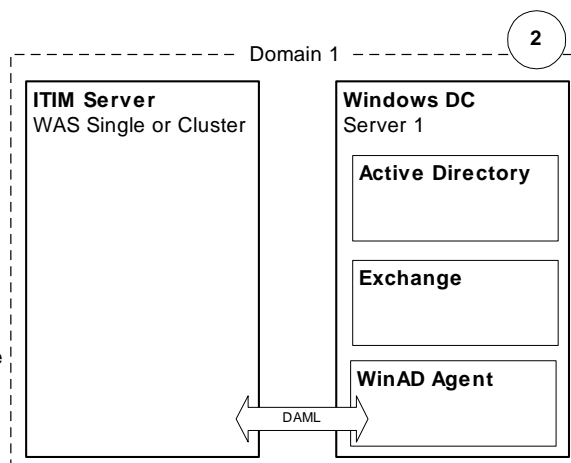


Scenario 1: Adapter deployed on WinAD DC w/o Exchange

Description: Deployment is typical of a Sales Demo on a VMWare image. Rarely used in client deployments. This is NOT a recommended setup since the adapter is local to the DC.

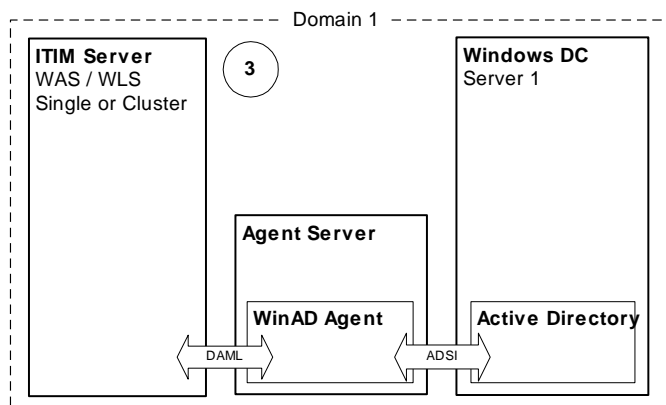
Scenario 2: Adapter deployed on WinAD DC w/ Exchange

Description: Deployment is typical of a Sales Demo on a VMWare image. Rarely used in client deployments. This is NOT a recommended setup since the adapter is local to the DC.



Windows Active Directory Adapter

Deployment Configurations for Windows and Exchange 2000 / 2003

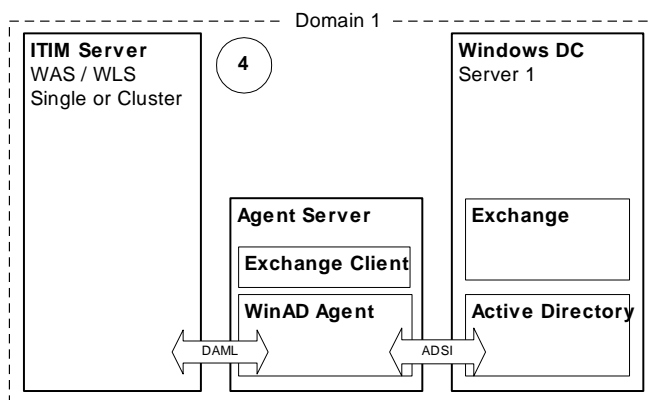


Scenario 3: Adapter on Adapter Server w/o Exchange

Description: Deployment is typical of a simple PoC or Client Test Environment where client is using Notes instead of Exchange. This is a recommended deployment.

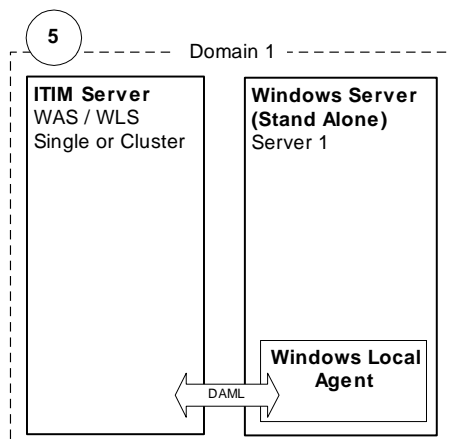
Scenario 4: Adapter on Adapter Server w/ Exchange

Description: Deployment is typical of a simple PoC or Client Test Environment where Exchange is used. This is a recommended deployment.



Windows Active Directory Adapter

Deployment Configurations for Windows and Exchange 2000 / 2003



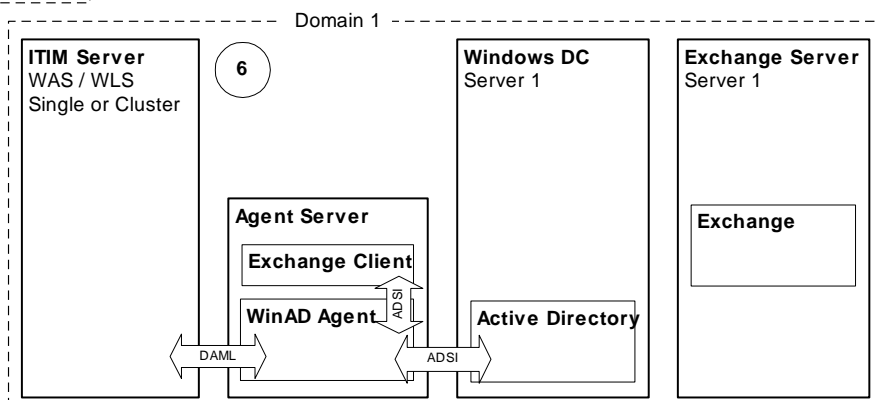
Scenario 5: Adapter on Stand Alone Server w/o AD

Description: Deployment is typical of a simple PoC without Active Directory. Used in some client environments to manage local accounts on stand-alone Windows servers. This is a recommended deployment for managing Local Accounts on non-Active Directory servers. One adapter is required on each stand-alone server.

Note: Windows Local Account Agent (formerly NT Agent) is used.

Scenario 6: Adapter on Adapter Server w/ Exchange

Description: Deployment is typical of a simple PoC or Client Test Environment where Exchange is used but neither AD nor Exchange are replicated. This is a recommended deployment.

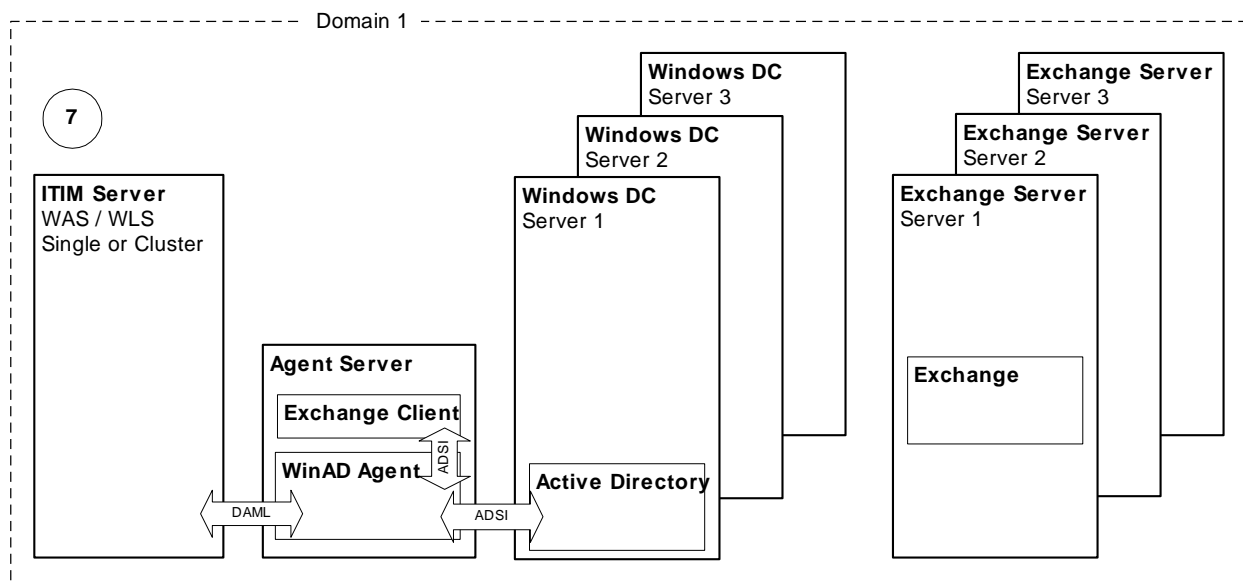


Windows Active Directory Adapter

Deployment Configurators for Windows and Exchange 2000 / 2003

Scenario 7: Adapter on Adapter Server w/ Replicated Active Directory and Exchange

Description: this is the first scenario that represents a production-grade Client deployment. This configuration is typical of a small to medium sized company with a single Windows Domain and several remote sites. The adapter is deployed on an Adapter Server so that if a DC drops off line, it can fail over (via ADSI) and send updates to one of the remaining DCs. This is a recommended deployment.

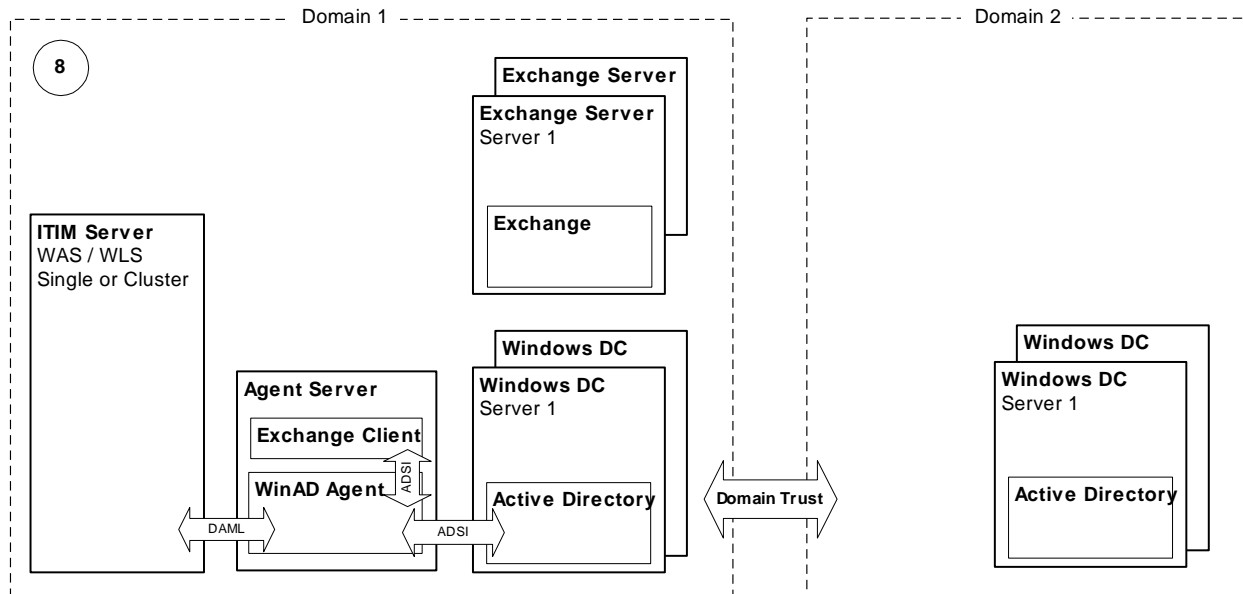


Windows Active Directory Adapter

Deployment Configurations for Windows and Exchange 2000 / 2003

Scenario 8: Adapter on Adapter Server in Multi-Domain Active Directory

Description: this represents a production-grade Client deployment with multiple domains. This configuration is common at medium to large sized companies with multiple Windows Domains and several remote sites. The adapter is deployed on an Adapter Server within one of the domains and can provision cross-domain to the second domain. Cross-domain trust is required and domains must be independent peer domains (e.g. no shared user or group objects). Within Identity Manager, there are two Services, one representing each domain. This is a recommended deployment for multi-domain situations.



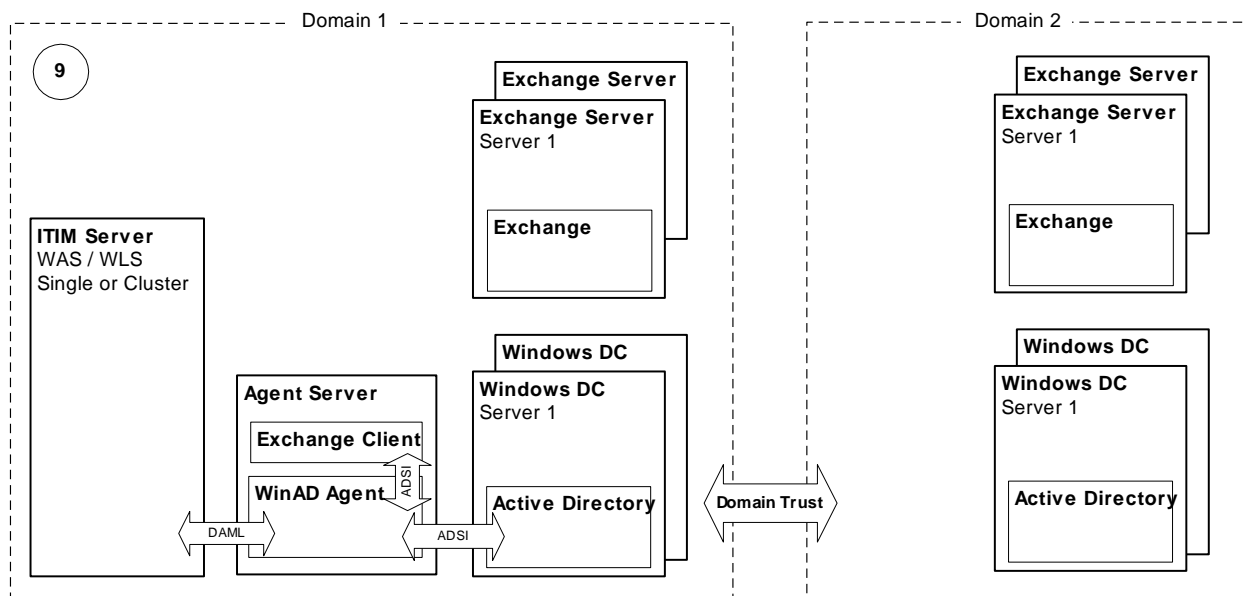
Windows Active Directory Adapter

Deployment Configuratons for Windows and Exchange 2000 / 2003

Scenario 9: (NOT SUPPORTED) Adapter on Adapter Server in Multi-Domain Active Directory w/ Multi-Domain Exchange

Description: this represents a production-grade Client deployment with multiple domains. This configuration is not supported. The supported configuration for this scenario requires two agents - one agent in each domain (Scenario 7)

This scenario includes both multiple Active Directory domains and multiple Exchange domains (e.g. IBM.com and Lotus.com). The adapter is deployed on an Adapter Server within one of the domains and can provision cross-domain to both the second AD and Exchange domains (cross domain trust is required). Within Identity Manager, there are two Services, one representing each domain.

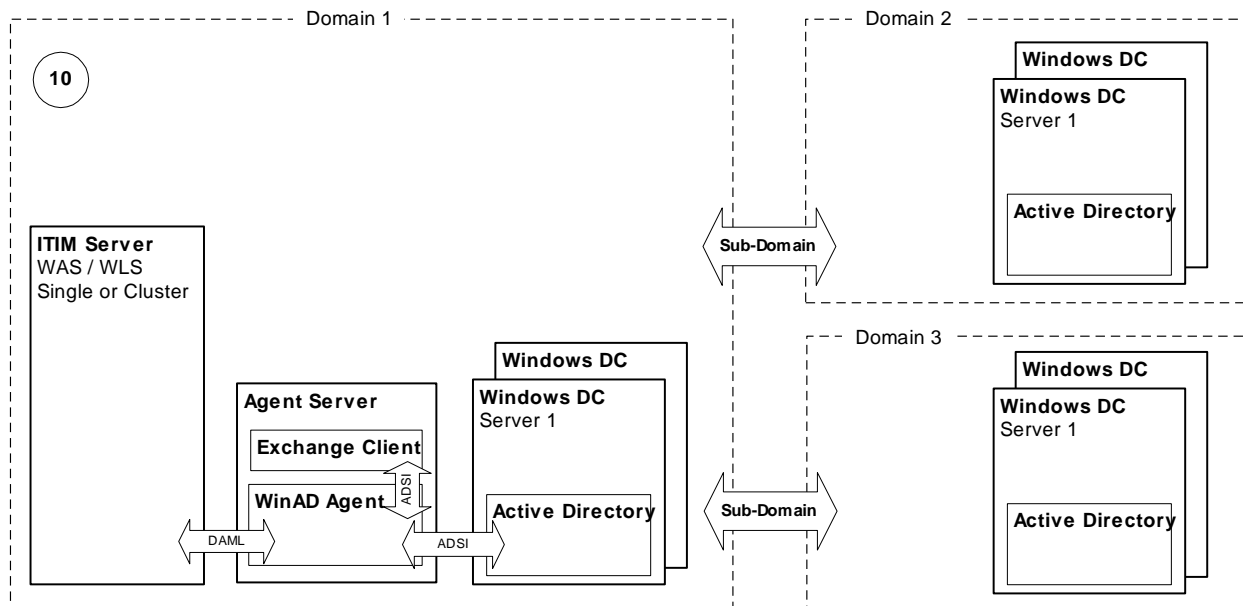


Windows Active Directory Adapter

Deployment Configuratons for Windows and Exchange 2000 / 2003

Scenario 10: (NOT SUPPORTED) Adapter on Adapter Server in Sub-Domain Active Directory

Description: this represents a production-grade Client deployment with multiple sub-domains. This configuration is not supported. Placing a WinAD in each domain may work in this environment if each of the domains is self contained (i.e. all groups and users referenceing those groups, are within the same domain), however, this is not typical. Nested domains usually share group references between domains and, therefore, must be managed as a whole. Due to the sharing of object references, there is no supported configuration available at this time.

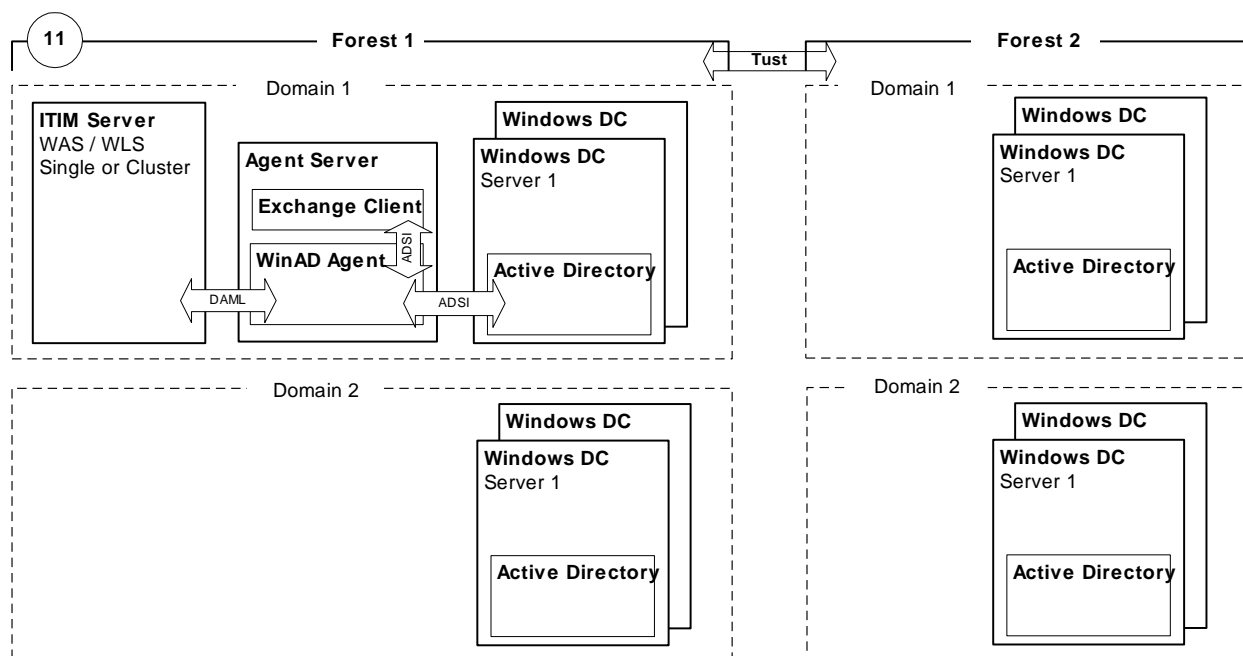


Windows Active Directory Adapter

Deployment Configuratons for Windows and Exchange 2000 / 2003

Scenario 11: (NOT SUPPORTED) Adapter on Adapter Server in Multi-Forest Active Directory

Description: this represents a production-grade Client deployment with multiple forests. This configuration is not supported. Each Forest must be managed separately even if trust relationships are established. The supported configuration for this scenario requires multiple agents - at least one agent per forest (Scenario 7 or Scenario 8).



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:

AIX
DB2
IBM
IBM logo
SecureWay
Tivoli
Tivoli logo
Universal Database
WebSphere

Lotus is a registered trademark of Lotus Development Corporation and/or IBM Corporation.
Domino is a trademark of International Business Machines Corporation and Lotus Development Corporation 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.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

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

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

End of Release Notes