Release Notes

IBM® Tivoli® Identity Manager

Unix and Linux Adapter

Version 4.6.22

Tenth Edition (September 30, 2010)

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

Contents

Preface

Welcome to the IBM Tivoli Identity Manager Unix and Linux 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 Unix and Linux Adapter Installation and Configuration Guide

Adapter Features and Purpose

The Unix and Linux Adapter is designed to create and manage accounts on AIX, Solaris, HP-UX, SLES and RHEL systems. The adapter runs in “agentless” mode and communicates via SSH to the Unix and Linux systems being managed. This Adapter does not create or manage systems running in NIS or NIS+ modes.

IBM recommends the installation of this Adapter (and the prerequisite Tivoli Directory Integrator) on each node of an Identity Manager WAS cluster. A single copy of the adapter can handle multiple Services of similar or varied Unix or Linux types. The optimum 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 Policy, Organization & Administration Guide for a discussion of these topics.

The Unix and Linux Adapter is a powerful tool that requires Administrator Level authority. The Adapter operates much like a human system administrator, creating accounts 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	September 30, 2010
Adapter Version	4.6.22
Component Versions	Adapter Build: 5.1182 Profile: AIX Profile 5.0.1008 Solaris 5.0.1008 Linux 5.0.1008 HP-UX 5.0.1008 Connector: 5.1182 Dispatcher: 5.123 or higher (packaged separately)
Documentation	Unix and Linux Adapter Installation and Configuration Guide v4.6.0 SC32-1755-02

New Features

Enhancement # (FITS)	Description
	Items included in current release
N/A	Added support for installation in AIX WPAR.
N/A	Installer updated from ISMP to InstallAnywhere. The Dispatcher is no longer automatically installed by the Unix/Linux adapter and must be installed separately.
	Items included in 4.6.21 release
N/A	Enhance the UnixLinux adapter to optionally terminate user session when user is suspended. See additional information in “Configuration Notes” section of this document.
	Items included in 4.6.20 release
MR1121083313	Unix/Linux: adapter should return exact OS error message when add request fails due to a duplicate UID. This Enhancement has been already provided for Solaris, Linux, and HPUX systems in earlier release. This version of the POSIX adapter is enhanced to reflect the exact system message when the user add request fails either due to duplicate ID or duplicate username.
MR0513095642	Unix/Linux: Need the Unix Posix Adapter to support DSA Keys instead of RSA keys. The Key based authentication is already supported by posix adapter. Earlier only RSA key based authentication is supported. This version of the POSIX adapter is enhanced to add the support for DSA Key-Based authentication. For Details of usage, plz check the "Updates to install guide" section at the End of the readme.
N/A	Unix/Linux: Enhanced adapter reconciliation performance for Aix, HPUX, Linux and Solaris systems. In this version of the adapter,Recon scripts for Aix, HPUX, Linux and Solaris systems have been changed to enhance the reconciliation performance.
N/A	Unix/Linux: removing adapter specific utility dependency from Dispatcher. The enhancement is to remove the adapter dependency from Dispatcher. The class files for the utile file PosixAdapterUtils.java. will now be bundled with the connector jar - posixconnector.jar.
N/A	Unix/Linux: removing posix connector dependency from Dispatcher. In the earlier version of adapter the connector used few constants from dispatcher related classes. These constants have now been included in connector so that to remove the dependency from dispatcher.

Enhancement # (FITS)	Description
	Items included in 4.6.19 release
MR0320094354	Unix/Linux: Enhance UnixLinux adapter to be able to work with additional Linux OS versions - Debian Linux. This version of the POSIX adapter is enhanced to support DEBIAN Linux version 5.0. The adapter has been certified with DEBIAN Linux version 5.0.2.
OSDB	Support for SLES 11
MR0218094115	Unix/Linux: Posix Adapter to use private/public keys without a passphrase. This version of the POSIX adapter is enhanced to use private/public keys without a passphrase. Note : Adapter will allow an empty passphrase to be used while Key Based Authentication is used as the authentication method.
MR0420095941	UnixLinux Adapter: Support of the AIX account attribute "hostsallowedlogin" and "hostsdeniedlogin" This version of the POSIX adapter is enhanced to support two new AIX attributes, named "hostsallowedlogin" and "hostsdeniedlogin". Please refer to AIX documentation for more details on these attributes. See Configuration Notes for more information.
MR0904095127	Sudo access should not be required for grep command. This version of the POSIX adapter is enhanced to work without requiring SUDO access on GREP command. From this release onwards, POSIX adapter will not require GREP command to be put in SUDOERS file.
MR0908096656	Solaris Posix Adapter does not create Home Directory based on Default Parent Directory as specified on Solaris Server configuration. See Configuration Notes for more information.
MR0921095040	The adapter should not try to execute any script from /tmp directory This version of the POSIX adapter will provide an option for the users to change the default location where the adapter script will get copied. See Configuration Notes for more information.
MR0918093229	Get Status from Pre-Post exec script execution. See Configuration Notes for more information

Enhancement # (FITS)	Description
MR0921095854	POSIX adapter SUDO setup should not require "echo" command to be part of SUDO list. This version of the POSIX adapter is enhanced to work without requiring SUDO access on ECHO command. From this release onwards, POSIX adapter will not require ECHO command to be put in SUDOERS file.
N/A	Enhanced adapter reconciliation performance for Linux systems. In this version of the adapter, Linux Recon scripts has been changed to enhance the reconciliation performance.
N/A	Configure Solaris adapter to not prompt for a new password when restoring account to support new functionality provided by Solaris 10. This version of the adapter will allow the user to restore an account without providing a password while restoring the account. After the account is being restored, the owner of that account can login to the target system using it old password.
	Items included in 4.6.18 release
MR0206092518	Enhance the adapter to support usernames longer than 8 characters. This feature is supported only on AIX v5.3 onwards. See the “Installation Guide” section of this document for more information.
MR1126085319	Enhance adapter to work with HP-UX trusted mode password prompts.
MR0611084354	Reset “failed login attempts” count on Linux This is a new feature that has been added in this release for Linux systems. With this feature, after every Password change operation and Restore operation, adapter will automatically reset the "Unsuccessful Login Count" of users to 0. Note: Adapter will not set "Unsuccessful Login Count" to 0, in case user is already active on resource while restore operation.
MR0130085348	Enhance the adapter to include the “unsuccessful max login count” on Linux (similar to umaxlntr to hpux) This is a new feature that has been added in this release of adapter. This feature can be used to set "Maximum Login Retries" for any user on Linux systems. See the “Installation Guide” section of this document for more information.

Enhancement # (FITS)	Description
	Items included in 4.6.17 release
	None
	Items included in 4.6.16 release
MR1110086153	Enhanced the Unix/Linux adapter to support a timeout (RXA timeout) See “Configuration Section” in this document for additional information.
MR072808316	Added a configuration option to the Unix/Linux adapter to turn off the "user private group" See “Configuration Section” in this document for additional information.
N/A	Add dispatcher enhancements to service form: Three dispatcher parameters are added on the service form. These attributes are: -> Disable AL Cache -> AL File System Path -> Max Connection Count See “Configuration Section” in this document for additional information.
N/A	Query on AIX group and ALL option: In the earlier version of Unix/Linux adapter (i.e. 5.107), when customer reconcile the data from any AIX resource, along with other groups one dummy group, named "ALL", gets reconciled which was used as a value of Sugroups attribute while adding a user. In this release of adapter(5.108), this is option is excluded. No "ALL" group will get reconcile. If user wants to gives the value of sugroups attribute as "ALL", he/she can just send an empty value for sugroups and resource automatically add "ALL" as the default value of sugroups.
	Items included in 4.6.15 release
N/A	Added support for RHEL 5

Enhancement # (FITS)	Description
	Items included in 4.6.14 release
N/A	AIX 6.1 Certification. Support for Aix 6.1
MR021308335	Enhance the adapter to bypass invalid password file entries. Invalid entries are skipped by connector and message logged in ibmdi.log. Recon will continue. Invalid entries will not be returned to ITIM. RECON status will still show SUCCESS. Invalid entry details can be found in ibmdi.log. (PMR 00140,SK5,649) See additional information in the Configuration Section of this document.
N/A	Additional Usability Enhancements: (1) Warning for non-supported OS levels See additional information in the “New Adapter Features” section. (2) Externalize the "Password prompt" strings See additional information in the “New Adapter Features” section. (3) Add postExec/preExec mapping in AL (see additional note 4 below) See additional information in the “New Adapter Features” section. (4) Enable debugging in sshConnection.java
	Items included in 4.6.13 release
	None
	Items included in 4.6.12 release
MR0130086950	Enhanced the adapter to include control for duplicate UIDs on Linux platforms.
MR0130084651	Enhanced the error messages returned for HPUX and added additional details when they are available from the OS.
	Items included in 4.6.11 release
N/A	Adding support for RedHat v5.0 Linux (RHEL v5.0)
MR1222065555	Adding support for umaxlntr attribute on HP Trusted machines
	Items included in 4.6.10 release
MR0430073532	AIX adapters should support rename when registry is files. Modification of UID is now allowed on AIX.

Enhancement # (FITS)	Description
	Items included in 4.6.8 release
	Added support for SLES 10.
	Added support for TDI 6.1.1
	Items included in 4.6.6 release
	None
	Items included in 4.6.5 release
	None
	Items included in 4.6.4 release
N/A	Support for TDI v6.1
MR0908065840	Enhance unix/posix adapter to support sudo-like connectivity option. See Installation Guide “Appendix B: Creating a Super User”
MR0522062817	Unix/Linux: remotely manage linux as non-root user See Installation Guide “Appendix B: Creating a Super User”
MR0426062649	Unix/Linux: Adapter needs to be able to run as a non root account See Installation Guide “Appendix B: Creating a Super User”
N/A	Enhance the adapter to support LDAP registries on AIX systems.
N/A	Enhance the adapter to support Certificate-based SSH connections. See Installation Guide “Appendix C: Key-based Authentication”
N/A	Enhance the adapter to support SSH 2.0 connections.
	Items included in 4.6.3 release
	None
	Items included in 4.6.2 release
N/A	N/A Unix/Linux adapter now supports the following new AIX attributes: RSS – Soft/Hard limits for physical memory. NoFiles – Soft/Hard limits for the number of file descriptors.
	Items included in 4.6.1 release
	None
	Items included in 4.6.0 release
	New adapter.

Closed Issues

Internal#	APAR#	PMR# / Description
		Items closed in current version
	IZ82811	28854,487,000 Unix/Linux adapter does not have correct TIM 4.6 server version requirements. Should list TIM Fix Pack 85.
	N/A	PMR 37391,487,000 - Unix/Linux issues with AIX & LDAP_AUTH The earlier version of the adapter was using CHSEC command to reset attribute unsuccessful_login_count=0 for AIX LDAP users. CHSEC command is not intended for the remote users and it is designed for the local users only. This version of the POSIX adapter uses CHUSER command to reset attribute unsuccessful_login_count=0 for AIX LDAP users.
	N/A	PMR 50664,499,000 Posix AIX recon on AIX machine with 20000 accounts takes too long. In this version of the adapter,Recon scripts for Aix system have been changed to enhance the reconciliation performance.
	N/A	N/A RXA timeout option not consistent on all the profiles. RXA timeout option was not present on service form of ITIM 5.1 profiles. Whereas it was present on service form for 46 and 50 profiles. In this release, ITIM 51 profiles has been changed to display the RXA timeout option on the service form.
		Items closed in 4.6.21 version
	IZ75546	PMR 31640,004,000 at.allow/at.deny/cron.allow/cron.deny corruption when deleting accounts. See additional information in “Configuration Notes” section of this document.
	IZ76603	15219,999,000 Path to faillog used by ITIM adapter in release notes should be updated. See additional information in “Configuration Notes” section of this document.
	IZ73366	94202,100,838 UNIXPOSIX ADAPTER 5.0.11 FAILS RECONCILING GROUP-ID ON AIX-LDAP See additional information in “Configuration Notes” section of this document.
	N/A	N/A On Aix CHSEC command is getting fired twice while restore operation.

Internal#	APAR#	PMR# / Description
	N/A	N/A On HPUX, if Home Dir Val contains double quotes, then adapter returns failure but resource add the account without a home dir. See additional information in “Configuration Notes” section of this document.
	N/A	N/A Adapter hangs when a group name with “()” is associated with user in useradd request. See additional information in “Configuration Notes” section of this document.
	N/A	N/A Adapter returns failure while suspending a suspend user and restoring an active user. See additional information in “Configuration Notes” section of this document.
	N/A	N/A Linux NonShadow:- Adapter should reconcile suspended account as suspended and active account as active See additional information in “Configuration Notes” section of this document.
	N/A	N/A If homedirectory contains space then it is not able to set umask,change homedirectory permission and can't delete homedirectory. See additional information in “Configuration Notes” section of this document.

Internal#	APAR#	PMR# / Description
		Items closed in 4.6.20 version
	IZ65609	90822,070,72 Adapter for Unix/Linux Could not set umask The earlier version of the adapter could not set the umask value in the profile file with sudo user. As the profile file existence check is performed by RXA and the RXA API's do not provide support for SUDO. The Fix for this is provided by replacing the RXA file existence API.
	IZ64091	06584,035,724 Special characters in gecos field cause exception in posix connector and recon to fail. The earlier version of the adapter could not recon the special characters in gecos field if the characters are from some Locale other than English. This version of the POSIX adapter is enhanced to reconcile the user data that contain special characters, i.e. characters from some LOCALE other than English. Prerequisites: 1. This feature is needed to be used mainly for non English Locales. For Locale with English no additional set up is required. 2. The default value if no value is supplied is UTF-8. 3. The system where ITDI Dispatcher is running must have the required CodePage, e.g. if Locale/Language on target system is German and ISO-8859-1 has been used for encoding in adapter then ISO-8859-1 must present on the system where ITDI Dispatcher is running.
	N/A	25190,370,000 Display non-zero return code in log after password change fails. The earlier version of the adapter was showing incomplete error message if the password change operation fails. The fix is provided by adding the return code value of the operation in the error message.
	IZ70478	46974,122,000 Home Directory group owner on Solaris should be primary group. The fix is provided so that the home directory owner is set to the primary group instead of default. The Fix is also provided for Linux systems. Note:- If either of home directory/primary group is invalid then both the attributes will not be set and get a warning, but user will be created.
	N/A	N/A Missing # sign to comment out the second line in LinuxShadowPConnRes.sh

Internal#	APAR#	PMR# / Description
36484		46118,487,000 UnixLinux adapter not reconciling erpasswordmaxage = -1 on Solaris. Earlier version of the adapter was not reconciling the negative values for the password age related attributes for the Solaris system. The fix is provided for all the password age related attributes for Solaris. i.e erPosixMinPwdAge, erPosixMaxPwdAge, erPosixPwdWarnAge, erPosixIdledays The fix is also provided for other platforms with the respective attributes and fix details as below: Aix: The fix is provided to set the least allowed value for this attribute is -1. erPosixPwdWarnAge Linux: The fix is provided to set the least allowed values for all these attributes is -1. erPosixMinPwdAge erPosixMaxPwdAge erPosixPwdWarnAge HPUX: The fix is provided to set the least allowed values for all these attributes is -1. erPosixMinPwdAge erPosixMaxPwdAge
		Items closed in 4.6.19 version
	IZ57781	15535,004,000 - City Public Service Problems with erPosixForcePwdChange attribute. CAUTION: The return value of the attribute "erPosixForcePwdChange" will be affected from this release of adapter forward. Please check compatibility with your Provisioning Policies before installing this version of the adapter. Adapter will return either TRUE or FALSE depending on the value of this ADMCHG flag on the target AIX system. If ADMCHG flag is set on the system for that user then it will return TRUE otherwise FALSE. It will never return a null value. The earlier version of the adapter was returning null if ADMCHG flag was not set on the target system.
	IZ65638	60280,6X8,760 The Unix/Linux adapter occasionally misidentified target OS type. Earlier version of the adapter sometimes misidentified the target OS type. This problem has been observed with TDI Fix Pack version 5 and above. This problem has been fixed in this version of the adapter.

Internal#	APAR#	PMR# / Description
	N/A	01689,6X1,760 PREEXEC and POSTEXEC don't work on DELETE operation of Posix UnixLinux Adapter. In this version of the adapter, option to execute "Pre-Exec and Post-Exec commands" is made configurable. Users can make use of this feature, if required. See Configuration Notes for more information
36468		N/A If password attribute is not present on restore, Posix Solaris adapter should not delete old password of user on Solaris version less than 5.10. Earlier version of the Posix adapter restores the user by deleting its password while restoring the account if password is not present in the Restore request, on Solaris 5.8 & 5.9 systems. This defect has been addressed in this release of the adapter. From this release onwards, adapter will not restore the user if password is not present in the Restore request and it will abort the retore request with an error message "No password specified. Restore operation cannot proceed on Solaris version below than 5.10" Note: Password is required while restoring the account only on Solaris versions below than 5.10. Restore operation can continue without a password on Solaris 5.10 systems.
		Items closed in 4.6.18 version
	IZ55495	26800,694,760 Warning occurs while changing password on AIX "root" account. Adapter returns a warning when changing the password of ROOT user through a SUDO/Super user. See the “Configuration” section for more information.
	IZ52238	77301,228,631 Negative value not allowed in POSIX values. Earlier version of adapter did not allow user to reset passwd aging on Solaris by setting -1 value for Max Password Age attribute. Removed UI constraint.
	N/A	54343,000,000 Clear force password change on AIX modify operation. On AIX, earlier versions of adapter were not able to clear the "Force Password Change" flag for users on modify operation. If an account is created with "Force Password Change" checkbox on then, on modify with "Force Password Change" checkbox unselected, adapter was not clearing this flag on resource.

Internal#	APAR#	PMR# / Description
	IZ50821	54067,6X8,760 Warning occurs when trying to create an HP-UX or Solaris account with UMASK attribute. The earlier versions of adapter prompts a warning when, through SUDO user account, it tries to add user on SOLARIS & HPUX with UMASK attribute. See the “Configuration” section for more information.
	IZ53507	54040,033,000 UID for 'NOBODY' displays in TIM as -2, but the number in /ETC/PASSWD is 4294967294.
	IZ52378	51106,025,724 Missing commands in install guide. See updates in the “Installation” section for more information.
	IZ55238	35585,999,000 AIX Sudo User and key file configuration. This was a documentation defect. The keygen program must be run when logged in as the user who will use the key. See “Installation Guide” section for more information.
	N/A	36260,033,000 Error during Linux recon. This was a documentation defect. Customer faced an issue due to a change in the format of /etc/passwd file. See “Configuration” section for more information.
	IZ53837	54256,033,000 Documentation defect. Some of the "OPTIONAL FEATURE" section information was missing in 2.1 version of the Developers Reference Guide (IM50-TDI-RMI-ADAPTER-DEVREF.PDF). The updated document is shipped with this adapter.
	N/A	Internal Defects: • Adapter Installer GetVersion bean failed on FP1 installation. Installer was going for update every time the user ran it, even if the installed connector version is same as the connector going to be installed. • Language properties file for Dispatcher/POSIX missing some properties. • Not able to modify home dir on AIX LDAP Home directory of the user. • Spelling errors in logged messages. • Secondary groups were not getting reconciled with non-shadow script.

Internal#	APAR#	PMR# / Description
		Items closed in 4.6.17 version
	IZ42244	53057,6X8,760 RESTORE operation to AIX account that isn't locked on the local machine will add ADMCHG flag to the account.
	IZ43344	03858,6X1,760 "staff" is set to group that is allowed to access to Home directory, not the owner's primary group.
	IZ47478	51125 Adapter not reconciling SYSTEM attribute correctly if it has spaces. Resulting in empty error message on completion of Recon.
	IZ38971	35800,033,000 AIX recon error with 5.3 ML7
	IZ48194	56928,SGC,724 Doc error in sudo user paths for Linux Systems.
34937		CMVC 34937 - Maximum days after expire value 000000.
34938		HPUX11iv3 Passwd Max/Min Age -1 after recon
34939		HPUX11iv3 pwd max age on system gets set to min in itim
34099		Unix/linux adapter install on win2k3 not correctly setting path. (Applicable for only windows and Aix)

Internal#	APAR#	PMR# / Description
		Items closed in 4.6.16 version
	IZ41653	55497,228,631 Restore operation not working correctly. This is a documentation defect. Before setting the property password_not_required_on_restore to true, verify that the system supports restore without a password for e.g. solaris 9 does not support this feature.
	N/A	N/A POSIX Installer does not remove the ITIMAd script while un-Installing the adapter on Aix. In the earlier version of Unix/Linux adapter (i.e. 5.107), when customer uninstalls the adapter, ITIMAd script was not removed by adapter. In this release of adapter(5.108), this issue has been fixed.
		Items closed in 4.6.15 version
	IZ30567	56327,999,866 Issue on Aix 6.1 with role accounts. The /etc/security/roles file on Aix 6.1 contains comments at top of file which gets reconciled as roles when reconciling support data.
	IZ32531	33450,025,724 Issue with gecos attribute on Aix. If the user gecos attribute value contains data as '=' character, then in recon the data after '=' character gets skipped by connector.
	IZ31905	66237,499,000 On some setups of Aix 5.2 machines, suspend operation failed because the "lsuser -R files -a account_locked <uid>" command did not retrieve the account_locked attribute.
	N/A	34013,101,616 Added support for RHEL5
	IZ34185	52416,6X8,760 PosixAdapter 4.6.14 - AIX does not delete an account when account creation fails due to passwd command not workg as expected. Adding user and changing it's password is an atomic operation. If password change command failed then account added was not being deleted.
	N/A	N/A Supports new dispatcher feature - Disable AL caching for a particular service.

Internal#	APAR#	PMR# / Description
		Items closed in 4.6.14 version
	N/A	28494,004,000 UnixLinux - recon errors. Note: /tmp folder must have 777 permission to perform reconciliation using sudo user. See Configuration Notes for additional information.
	IZ17739	69855,033,000 28960,004,000 75702,000,738 Recon hangs on AIX. Recons failing sporadically and do not finish.
	N/A	N/A Lifetime and idle days attributes not getting cleared on HPUX.
		Items closed in 4.6.13 version
	IZ22393	25005,707,707 Problem changing passwords on RedHat EL 3 U7 AS
		Items closed in 4.6.12 version
	N/A	34846,019,866 POSIX hang on AIX. Transactions that suspend multiple accounts are not completing.
	IZ12686	69258,073,649 Issue with password prompt. Operations hang. Posix adapter deletes fail randomly on HP-UX trusted systems.
	IZ17040	69416,073,649 Random transactions hanging. Recon hang. Unable to change password with Unix/Linux adapter on AIX v5.2.
	IZ17739	69855,033,000 Issue with multiple RECONs. Hanging threads
	N/A	67196,070,724 Multiple recons hang and produce an eventual Out of Memory error.
	AZ4961	69413,073,649 issue with dup uid on linux (See also MR0130086950)

Internal#	APAR#	PMR# / Description
	IZ13066	55875,070,724 Regarding "staff" group on AIX, "other" on Solaris. The default “staff” and “other” groups are added to the account upon creation.
	AZ4961	69414,073,649 Error messages returned for HPUX are not as detailed as other Unix versions (See also MR0130084651)
	IZ16582	77114,033,000 erPosixpwdLastChangeDate fix put in UnixLinux version 5.014 (release 4.6.11) does not work correctly
	N/A	N/A - PATH variable added to Posix installer to pick 3rd party dll. - RHEL30 Update 8 - password prompt support - Typo in syntax of erPosixTrustedPath attribute in Aix schema.dsml file - Changes in ITIMAd script for Solaris restrictions
		Items closed in version 4.6.11 version
	IZ15500	69175,073,649 Adapter installer includes the wrong version of the PosixConnector.jar for use with TDI 6.1.
	IZ00030	N/A Service name must not contain a slash (/). Added constraint to the TIM UI form. Applies to: Solaris, AIX, Linux, HP-UX.
	IZ12686	69258,073,649 Delete user request hangs for HP-UX Trusted resource. May occurs on slower network segments hosting any Unix or Linux system (not only HP-UX).
	IZ14628	69422,073,649 Modification of attribute Account Expiration Date fails for HPUX Trusted. The adapter should remove the expiration date (set it back to “never”) if a null is received.
	IZ10781	59552,033,00/IZ10781 Add support for erPosixPwdLastChange on Aix.
31707	N/A	(internal) 1. Fixed Home Directory deletion issue with HPUX 2. UnixLinux connector – correct handling of setshadow attributes 3. HP – Moved Trusted attributes to a 3rd Tab of the UI. 4. AIX – correct recon format of multivalued attributes.
27518	N/A	(internal) HPUX account expiration date. Changes in AL to be made in 4.6 profile - already made in 5.0 profile

DevTrack	APAR#	PMR# / Description
		Items closed in 4.6.10 version
N/A	IZ05364	83762,999,866 Bourne shell requirement is not listed in the Installation Guide. Fix: The requirement is now added to the "Corrections to Installation Guide" section of this document.
29920 29464 29667 30791 30791 30791 30791 30791 30791 30791 30791		Release 5.011 Nov 02 2007 (ITIM50) (Profile Defects) ▪ Aix recon fails if there are large number of groups ▪ Make erPosixUseSudo required=false in Linux profile ▪ Account Add remains in pending of special characters ▪ Changed the syntax for UID and GroupId to string for Solaris, HP-UX and Linux ▪ Change recon script permissions from 777 to u+x ▪ Aix command executor, multi value attr setting error in the logic when done one at a time ▪ generateFilter() logic not correct - all accounts are retrived and sent to dispatcher (Unix Linux Installer defects) ▪ ITIMAd - stop src on Aix to get pid path searched is _jvm but this can be jvm depending on ITDI version ▪ During uninstall for non-windows when stopping service links are also removed ▪ After uninstall (only adapter is uninstalled) service is not restarted
27283 25750		Release 5.009 Aug 6 2007 (ITIM50) ▪ Recon not working for SUSE 10 POSIX Adapter ▪ Licence and License - spelling error in installer ▪ Removal of com.ibm.di.dispatcher.ssl.clientAuth=false from global.properties during uninstall.
27496 27512 27513 27523 27503 27521		Release 5.008 Jul 27 2007 (ITIM50) ▪ Account Expire Date HPUX defects - not reconciling, format wrong in add/mod, itim ldap ▪ erPosixPwdMaxAge does not get set on modify on HPUX. OK on add. ▪ Remove constraint of min value of 0 for attributes: erPosixMaxPwdAge and erPosixIdleDays in HPUX ▪ erposixmaxpwdage, erposixminpwdage, password warn age, idle days, force password change on HPUX - are not set properly on add/modify ▪ Changed the syntax for UID and GroupId to string for Solaris, HP-UX and Linux ▪ All shadow related attributes are kept on one tab of service form for HP-UX

DevTrack	APAR#	PMR# / Description
25879 25748 27278 23432 24362 42781 25427 25748 25801 25222 26054		Release 5.007 (ismp 11.5) Jul 20 2007 ITIM 50/ITIM46 (ismp 11.5) ▪ In itim_listener.properties, all comments should be updated to use "seconds" instead of "milliseconds". ▪ Adapter wizard install steps should be re-ordered. ▪ TDI Adapters fail to start using SSL authentication.Update com.ibm.di.dispatcher.clientAuth property in the solution.properties file. Release 5.007 (ismp 11.5) Jul 7 2007 ITIM 50/ITIM46 ▪ 64-bit machine installer does not work ▪ TDI on Aix cannot connect to ipv6 machine ▪ installer should create tim sol folder ▪ Test connection fails first time immediately after fresh install ▪ installer prompts for adap sol after confirmation panel - reorder the steps Release 5.007 June 25 2007 ITIM 50/ITIM46 itdi posix hpux recon data mismatch and errors No error displayed when uid entered as -ve Max pwd age, Min Pwd Age, Pwd Warn Age, Posix Idle Days allow -ve values MR0430073532 PMR 52467 allow eruid rename on Aix when registry is files
23406 24135 24400 24399 15349		Release 5.006 May 11 2007 ITIM 50 ▪ ITDI location is must for cluster setup ▪ Unknown group error during user add on Linux ▪ Dispatcher version should be displayed in the log ▪ Date format should be consistent across UnixLinux adapter ▪ Error{0} while adding existing user on linux machine
		Items closed in 4.6.9 version
C25801 C25222 C26054		TDI posix hpux recon data mismatch and errors No error message displayed when UID num is entered as -ve value Password maximum age accepts negative values.
		Items closed in 4.6.8 version
	IY97099	02895,033,000 UnixLinix Agent does not recon Gecos info when setup to run via sudo and the target platform is AIX. (Directory syntax returned to Character)
		Items closed in 4.6.7 version
	IY97099	02895,033,000 UnixLinix Agent does not recon Gecos info when setup to run via sudo and the target platform is AIX.

DevTrack	APAR#	PMR# / Description
		Items closed in 4.6.6 version
	IY97099	02895,033,000 UnixLinix Agent does not recon Gecos info when setup to run via sudo and the target platform is AIX.
	IY96399	15641,101,616 Using adapter to modify modify Directory permission fails (‘|’ missing).
	IY96394	15697,101,616 POSIX Connector cannot name Home Directory (cannot rename home dir).
		43897,227,000 Linux Profile Upgrade issue. Profile does not load properly.
	IY96539	01096,370,000 Unix/Linux Adapter is not placing the UNIX scripts in the solutions directory during upgrade.
	IY96702	40824,999,866 Wrong path listed in the “Creating Super User on AIX” section. (See Configuration Notes below for the correction)
c22838 C22324 C23072	N/A	(internal pmr) POSIX Linux service creation fails if password is not provided. Problem stopping and starting Dispatcher on Solaris "ITIM Ad doesn't stop". ITIMAd stop does not stop the ITIDI instance on Solaris

DevTrack	APAR#	PMR# / Description
		Items closed in 4.6.6 version
N/A	IY95982 IY96702	43897,227,000 and 40824,999,866 Incorrect instructions for setting up the sudo account.
N/A	N/A	40825,999,866 POSIX AIX recon warning with group ALL, mismatch in profile for attribute erPosixGroupId.
N/A	IY95409	40825,999,866 Schema mismatch across various Unix profiles.
DT 17511	N/A	N/A HP Trusted - active/suspend issue - accounts reported as inactive during reconciliation.
N/A	IY93784	59579,033,000 Password change operation does not automatically reset the unsuccessful login count.
N/A	IY95389	58435,005,000 Dispatcher service stops after user logs off. NOTE: In order for the changes related to IY95389 (Dispatcher service stops after user logs off) to take effect, uninstall the previous version of the adapter and dispatcher and then install the new one. There were no changes to the java code only to the way the installer creates the windows service. The -xrs parmater was added to resolve the above issue.
		Items closed in 4.6.5 version
N/A	IY93650	73484,057,649 Posix Adapter not setting erPosixLastAccessDate on recon.
N/A	IY94318	41771,999,866 PosixAixProfile.jar Unable to render service form in ITIM GUI. Incorrect case of the profile file names.
N/A	N/A	N/A Updated RXA jars to Dec 14, 2006 maintenance pack. Resolves “connection hang” issues found in previous version.
N/A	IY93167	47629,005,000 Null pointer exception may occur if custom adapter assembly lines do not setting reason code on each results page.

DevTrack	APAR#	PMR# / Description
		Items closed in 4.6.4 version
		None
		Items closed in 4.6.3 version
C15373	N/A	N/A Add transaction may be fail but list a success if the Username contains spaces or special characters. but account is not actually created on the Unix system.
C15597	N/A	N/A If home directory includes an invalid partition, the creation of the Home Directory will fail and the OS may assign a default directory. The value of this default directory will not be known to ITIM, and will display as blank, until after the first Reconciliation.
		Items closed in 4.6.2 version
		None
		Items closed in 4.6.1 version
N/A	N/A	N/A Change to the directory OID for the adapter schema. **NOTE: special upgrade instructions apply. Please see "Corrections to Installation Guide" section below**.
		Items closed in 4.6.0 version
C15754	N/A	N/A When requesting an account, checking the "Allow at jobs" or "Allow cron jobs" checkbox causes subsequent requests to fail.

Known Issues

DevTrack	APAR#	PMR# / Description
		NOTE: the "Allow Duplicate UID" is a send-only attribute. The checkbox will be reset after a Reconciliation.
		Profile Import Error When importing any of the Unix/Linux profiles (AIX, Solaris, HPUX, Linux) on an existing system, you may encounter an error with the erPosixGecos attribute. The erPosixGecos attribute may have been defined as a "Binary" syntax on your previous setup, and it is defined as "Directory String" syntax with this release. Such errors can be safely ignored as the profile import will leave your erPosixGecos attribute definition as is.
		TDI Application Monitoring Console NOTE: when using the TDI Application Monitoring Console, the RMI traffic to TDI is rerouted to port 1099. This may affect the operation of the TIM TDI-based adapters. Two options are available: (1) Change the TIM Service form for the TDI-based adapters to specify port 1099 (instead of the default 16231, or (2) configure the Application Monitoring Console to listen on port 16231 by modifying the api.remote.nameing.port property in the solution.properties file.
		Changing Primary Group Values on AIX Value of primary group is reflected in the values of secondary groups after useradd/usermod operations for Aix. If primary group and secondary groups are modified in the SAME REQUEST, the new value of primary group is added to secondary groups but the old value of the primary group does not get removed from secondary groups list. Example: Assume that a user is added with two attributes Primary group = gr01, Secondary Groups = gr02,gr03 Then User is modified for the two attributes Primary group = grp1, Secondary Groups = grp2,grp3 Result: In this case on resource values of secondary group will be grp1,grp2,grp3,gr01.
		Reconciliations Hang on AIX The adapter has been designed to accommodate most configuration options for SSH. However, if you are running AIX 5.3 and experience hanging reconciliations, you may be required to upgrade SSH to version OpenSSH v4.7_r1. AIX Support recommends this version of OpenSSH.

DevTrack	APAR#	PMR# / Description
		Unlocking Accounts on Solaris 9 Solaris 9 does not have a method to unlock an account without supplying a new password. The adapter profile specifies the “Password Required on Restore” option. Changing the Restore options for Solaris 9 is not supported -- Solaris 9 password must always be required on restore.
		Password Change with using LDAP Option on AIX If multiple AIX services are setup to use LDAP, and each of these AIX services are using the same LDAP to store its users, then errors may occur when changing passwords from TIM if the LDAP is setup to use “password history checking.” The problem occurs when TIM is setup for password synchronization. TIM will send the same password to each AIX service and since all the services point to the same LDAP, the same password will be set twice, resulting in a history violation.

Installation and Configuration Notes

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

Corrections to Installation Guide

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

NOTE: Many of the closed APARs in this adapter rely on fixes in TDI v6.1.1 FP3.
The adapter now supports only the following versions of TDI:

- TDI 6.1.1 FP3 or later

Important Note regarding installer

1. Installer is now built using Install Anywhere (2009). ISMP use to build installer is discontinued from this release onwards.

2. The unixLinux installer will no longer install the dispatcher. Make sure that dispatcher is installed separately before you install UnixLinux.

Java Installation Option

This release contains an additional installation program not mentioned in the Installation and Configuration Guide. If you are running TDI on platforms other than Linux or Windows, please run the java-based install as directed below. Run this installation program on the server in which Tivoli Directory Integrator is installed.

PosixAdapterInstall.jar Installation program for other platforms.

NOTE: the PosixAdapterInstall.jar is a java-based installer. Please ensure that java is installed and properly configured for your system. Launch the install with the following command.

```
Java -jar PosixAdapterInstall.jar
```

Required SSH and Shell Versions

The Unix/Linux adapter is built on Tivoli Directory Integrator and uses the RXA component to establish the SSH connection to the systems being managed. RXA requires specific SSH and Shell versions for proper operation. These include:

- Bourne shell (/bin/sh) must be the default login shell for the account used by the adapter.
- OpenSSH must be the SSH package

Refer to the Tivoli Directory Integrator for additional details and package requirements.

SSH Configuration

UsePrivilegeSeparation must be set to yes in the sshd_config file otherwise the adapter account will be locked. The defaults value of UsePrivilegeSeparation is yes.

Upgrading from version 4.6.0 of this adapter

This version of the adapter has changed the OID (Object ID) of the adapter schema attributes. The prior version of the adapter schema must be removed before installing version 4.6.1 of the adapter.

If you are currently running ITIM Express version 4.6.0 (build 6006 Feb 28, 2006 GA), special upgrade instructions apply. Please contact ITIM Level 2 Support (800-IBM-SERV) to receive an upgrade script and additional instructions.

Support for SSH 2.0

Page 5 of Chapter 2 “Installing the Secure Shell protocol” incorrectly states that only v1.5 is supported. This version of the adapter supports SSH v1.5 and v2.0 (password and certificate).

Installing on zOS and zLinux

For installation of this adapter on zOS and zLinux, please refer to the document “RMI Adapters for zOS” and “RMI Adapters for zLinux” packaged in the /zSystem subdirectory of this release.

Creating a Super User on AIX Operating System

Corrected documentation (page 41 “Creating a super user on a AIX operating system“ Item 2b) needs to include a reference to “/usr/sbin/lsuser” and needs a slash (“/”) before usr/bin/cat. The section should read:

```
# User privilege specification
tdiuser ALL=NOPASSWD:
/usr/bin/pwdadm,/usr/bin/passwd,/usr/bin/mkuser,/usr/sbin/rmuser,/usr/b
in/chuser,/usr/bin/chmod,/usr/bin/cat,/usr/bin/echo,/usr/bin/grep,/usr/
bin/rm,/usr/bin/rmuser,/usr/bin/tee,/usr/bin/ed,/usr/bin/groups,/usr/bi
n/ls,/usr/bin/logins,/usr/sbin/lsuser
```

Creating a Super User on Solaris Operating System

Corrected documentation (page 42 “Creating a super user on a Solaris operating system“ Item 2b) needs to include a reference to “/usr/bin/ed” and should read:

```
# User privilege specification
tdiuser ALL=NOPASSWD:/usr/bin/passwd,/usr/sbin/useradd,
/usr/sbin/usermod,/usr/sbin/userdel,/usr/bin/tee,/usr/bin/egrep,
/usr/bin/chmod,/usr/bin/echo,/usr/bin/vi,/usr/bin/cat,
/usr/bin/logins,/usr/bin/ls,/usr/bin/ed
```

Creating a Super User on Linux

The documentation for 'Creating a Super User on Linux Operating System' for 4.6 and 5.0 references a command that does not exist or used (/usr/bin/logins) on Linux systems (RH4, RH5 and SLES10). this command should not be added in the sudoers file. It should read as following:

Insert the following lines to allow sudo access.

```
# User privilege specification
Tdiuser ALL=NOPASSWD:/usr/bin/passwd,/usr/sbin/useradd,
/usr/sbin/usermod,/usr/sbin/userdel,/usr/bin/tee,/bin/grep,/bin/chmod,
/bin/echo,/bin/vi,/bin/cat,/bin/ls,/usr/bin/chage,/usr/bin/groups,
/bin/ed
```

TDI Base Service support

The Dispatcher has been changed to use the native TDI installer. Please follow the steps below to install this new release of the Dispatcher.

I. The new Installer (5.014) will not work correctly on windows and Aix platforms, if the older version of Dispatcher/POSIX adapter is installed. You need to uninstall the previous Dispatcher/POSIX Installation and then freshly install the new dispatcher version (5.014).

II. This new Installer will copy the 3 new files in adapter solution directory folder (Windows Platform only).
a. ibmdiservice.exe
b. ibmdiservice.props
c. log4j.properties

III. After installing the adapter, default logs are at INFO level. To change log levels to DEBUG mode change the log4j.properties value from the adapter solution folder instead of adapter solution\etc folder file(Windows platform only).

IV. The Adapter service name is changed to "IBM Tivoli Directory Integrator (TIM Adapters)" on windows platform.

Starting and Stopping the Dispatcher on AIX Platforms

On AIX platforms, the dispatcher installer copies the ITIMAd script file to the Tivoli Directory Integrator adapter's solution directory. This directory is a separate solution directory for all Tivoli Directory Integrator-Based adapters. Run the following commands from the Tivoli Directory Integrator adapter's solution directory to start, stop, and restart the dispatcher service:

```
ITIMAd startsrc
ITIMAd stopsrc
ITIMAd restartsrc
```

SUDO/Super Account Setup

If Adapter is running from a SUDO/Super user account, following commands need to be there in that user's path.

"usermod.sam" command:
The full path of the command is "/usr/sam/lbin/usermod.sam"

This is command has been used to enhance the adapter to change the password of the root/super user on HP-UX Trusted systems. It should be there in SUDO.

Changes to Super User Setup

- (MR0206092518) If Adapter is running from a SUDO/Super user account, following commands need to be there in that user's path: "mv" command

  On AIX systems, the full path of command is "/usr/bin/mv"

- (IZ52378) Remove "vi" command from sudo-setup-config section of install guide (Appendix C. Creating a super user on a supported operating system) for all operating systems, as adapter is no longer using this command.

- Add "lsgroup" Command to sudo-setup-config section of install guide (Appendix C. Creating a super user on a supported operating system) as "/usr/sbin/lsgroup" is being used by adapter for AIX systems.

- (IZ52378) Add "chpasswd" Command to sudo-setup-config section of install guide (Appendix C. Creating a super user on a supported operating System) as "/usr/bin/chpasswd" is been used by adapter for AIX systems.

- (IZ52378) Add "lsuser" Command to sudo-setup-config section of install guide (Appendix C. Creating a super user on a supported operating system) as "/usr/sbin/lsuser" is been used by adapter for AIX systems.

- (IZ52378) Add "ed" Command to sudo-setup-config section of install guide (Appendix C. Creating a super user on a supported operating system) as "/usr/bin/ed" for Solaris, "/bin/ed" for RHEL systems & "/usr/bin/ed" SUSE systems.

- (IZ50821) If Adapter is running from a SUDO/Super user account, following commands need to be there in that user's path.

  "tee" command:
  On Linux systems, the full path of command is "/usr/bin/tee"
  On Solaris systems, the full path of command is "/usr/bin/tee"
  On HPUX systems, the full path of command is "/usr/bin/tee"

  "cp" command:
  On Linux systems, the full path of command is "/usr/bin/cp"
  On Solaris systems, the full path of command is "/usr/bin/cp"
  On HPUX systems, the full path of command is "/usr/bin/cp"

- (IZ55495) If Adapter is running from a SUDO/Super user account, following commands need to be there in that user's path.

  "chsec" command.
  On AIX systems, the full path of command is "/usr/bin/chsec"

- (36260,033,000) NOTE: POSIX adapter is highly dependent on format of /etc/passwd file. The adapter does not support modifications to the format of /etc/passwd file.

- (MR0130085348) If Adapter is running from a SUDO/Super user account, following commands need to be there in that user's path:

  "faillog" command.
  The full path of command is "/usr/bin/faillog"

- for AIX,Solaris and HPUX OS:(IZ75546)If Adapter is running from a SUDO/Super user account, following commands need to be there in that user's path:
  a) "mkdir" command
  b) "rm" command.

  Please specify full path of "mkdir" and "rm" command into sudoers file. for example on Aix mkdir command path is "/usr/bin/mkdir" and rm command path is "/usr/bin/rm"

- For AIX,Solaris, Linux and HPUX OS: (Kill active user process on suspending an account) If Adapter is running from a SUDO/Super user account, kill command need to be there in that user's path. The full path of the command is /usr/bin/kill.

Note:- The full path of command may vary from resource to resource .

Consolidated List of Changes to Super User Setup

NOTE: the commands listed in the sudo setup documentation are documented at their default locations. The locations are configurable and may change slightly from release to release. For example, in SLES 10 the location of the faillog is "/usr/bin" but in SLES 11 the vendor moved it to "/usr/sbin". Please check with your system administrator to validate the location of these binaries.

Following is the set of commands for 4.6 and 5.0 versions:

```
Aix
/usr/bin/pwdadm,/usr/bin/passwd,/usr/bin/mkuser,/usr/sbin/rmuser,/usr/b
in/chuser,/usr/bin/chmod,/usr/bin/cat,/usr/bin/rm,/usr/bin/tee,/usr/bin
/ed,/usr/bin/groups,/usr/bin/ls,/usr/bin/logins,/usr/sbin/lsuser,/usr/b
in/mv,/usr/sbin/lsgroup,/usr/bin/chpasswd,/usr/bin/chsec,/usr/sbin/user
mod,/usr/sbin/lsrole,/usr/bin/mkdir,/usr/bin/rm,/usr/bin/kill

Linux
/usr/bin/passwd,/usr/sbin/useradd,/usr/sbin/usermod,/usr/sbin/userdel,/
usr/bin/tee,/bin/chmod,/bin/cat,/bin/ls,/usr/bin/chage,/usr/bin/groups,
/bin/ed,/bin/cp,/usr/bin/faillog,bin/kill

Note: The complete path of "ed" command is "/bin/ed" for RHEL systems &
"/usr/bin/ed" for SUSE systems & "/bin/ed" for Debian systems.

Solaris
/usr/bin/passwd,/usr/sbin/useradd,/usr/sbin/usermod,/usr/sbin/userdel,/
usr/bin/tee,/usr/bin/chmod,/usr/bin/cat,/usr/bin/logins,/usr/bin/ls,/us
r/bin/ed,/usr/bin/cp,/usr/bin/mkdir,/usr/bin/rm,/usr/bin/kill

HPNTrusted
/usr/bin/chmod,/usr/bin/cat,/usr/sbin/logins,/usr/bin/ls,/usr/bin/passw
d,/usr/sbin/useradd,/usr/sbin/usermod,/usr/sbin/userdel,/usr/bin/tee,/u
sr/bin/ed,/usr/bin/cp,/usr/bin/mkdir,/usr/bin/rm,/usr/bin/kill

HPTrusted
/usr/bin/passwd,/usr/sbin/useradd,/usr/sbin/usermod,/usr/sbin/userdel,/
usr/bin/cat,/usr/lbin/getprpw,/usr/lbin/modprpw,/usr/bin/chmod,/usr/bin
/ls,/usr/bin/tee,/usr/bin/ed,/usr/sbin/logins,/usr/sam/lbin/usermod.sam
,/usr/bin/cp,/usr/bin/mkdir,/usr/bin/rm,/usr/bin/kill
```

Following is the set of commands for Identity Manager 5.1 version:

```
AIX
/usr/bin/pwdadm,/usr/bin/passwd,/usr/bin/mkuser,/usr/sbin/rmuser,/usr/b
in/chuser,/usr/bin/chmod,/usr/bin/cat,/usr/bin/rm,/usr/bin/tee,/usr/bin
/ed,/usr/bin/groups,/usr/bin/ls,/usr/bin/logins,/usr/sbin/lsuser,/usr/b
in/mv,/usr/sbin/lsgroup,/usr/bin/chpasswd,/usr/bin/chsec,/usr/sbin/user
mod,/usr/sbin/lsrole,/usr/bin/mkgroup,/usr/sbin/rmgroup,/usr/bin/chgrou
```

```
p,/usr/bin/mkrole,/usr/sbin/rmrole,/usr/bin/chrole,/usr/bin/mkdir,/usr/
bin/rm,/usr/bin/kill

Linux
/usr/bin/passwd,/usr/sbin/useradd,/usr/sbin/usermod,/usr/sbin/userdel,/
usr/bin/tee,/bin/chmod,/bin/cat,/bin/ls,/usr/bin/chage,/usr/bin/groups,
/bin/ed,/bin/cp,/usr/bin/faillog,/usr/sbin/groupadd,/usr/sbin/groupmod,
/usr/sbin/groupdel,bin/kill

Note: The complete path of "ed" command is "/bin/ed" for RHEL systems &
"/usr/bin/ed" for SUSE systems & "/bin/ed" for Debian systems.

Solaris
/usr/bin/passwd,/usr/sbin/useradd,/usr/sbin/usermod,/usr/sbin/userdel,/
usr/bin/tee,/usr/bin/chmod,/usr/bin/cat,/usr/bin/logins,/usr/bin/ls,/us
r/bin/ed,/usr/bin/cp,/usr/sbin/groupadd,/usr/sbin/groupmod,/usr/sbin/gr
oupdel,/usr/bin/mkdir,/usr/bin/rm,/usr/bin/kill

HPNTrusted
/usr/bin/chmod,/usr/bin/cat,/usr/sbin/logins,/usr/bin/ls,/usr/bin/passw
d,/usr/sbin/useradd,/usr/sbin/usermod,/usr/sbin/userdel,/usr/bin/tee,/u
sr/bin/ed,/usr/sbin/groupadd,/usr/sbin/groupdel,/usr/sbin/groupmod,/usr
/bin/cp,/usr/bin/mkdir,/usr/bin/rm,/usr/bin/kill

HPTrusted
/usr/bin/passwd,/usr/sbin/useradd,/usr/sbin/usermod,/usr/sbin/userdel,/
usr/bin/cat,/usr/lbin/getprpw,/usr/lbin/modprpw,/usr/bin/chmod,/usr/bin
/ls,/usr/bin/tee,/usr/bin/ed,/usr/sbin/logins,/usr/sam/lbin/usermod.sam
,/usr/sbin/groupadd,/usr/sbin/groupdel,/usr/sbin/groupmod,/usr/bin/cp,
/usr/bin/mkdir,/usr/bin/rm,/usr/bin/kill
```

Note:- The full path of command may vary from resource to resource.

Note: Following commands are used by the connector but are not needed in the sudoers file. However if sudo user is used, then the user needs execute permissions on these commands. The list of commands are :

```
Aix :
/usr/bin/tr, /usr/bin/cut, /usr/bin/grep, /usr/bin/egrep, /usr/bin/awk,
/usr/bin/sort, /usr/bin/ps, /usr/bin/sed

Linux:
/usr/bin/tr, /bin/cut, /bin/grep, /bin/egrep, /bin/awk ,/bin/sed,
/bin/sort, /bin/ps

Solaris:
/usr/bin/tr, /usr/bin/cut, /usr/bin/grep, /usr/bin/egrep, /usr/bin/awk,
/usr/bin/sort, /usr/bin/ps, /usr/bin/sed


HPUX:
/usr/bin/tr, /usr/bin/cut, /usr/bin/grep, /usr/bin/egrep, /usr/bin/awk,
/usr/bin/head, /usr/bin/sort, /usr/bin/ps, /usr/bin/sed
```

Note:- The full path of command may vary from resource to resource.

Key-Based Authentication
Refer to IZ55238 - PMR 35585.
The installation guide should read:

Appendix D : Key-based authentication for the UNIX and Linux Adapter:

(First point should be like this)
Use the ssh-keygen tool, while logged in as a user that is defined on the itim service form as administrator, to create a key pair.

(A NOTE should be added regarding Point 1.d to read as)

NOTE: Although the ssh-keygen will accept a blank passphrase, it is required on the ITIM service form.

Home Directory Permissions

Adapter needs "Home directory Permissions" as 755 to set the umask value. Adapter may not work as expected if SUDO user do not have permissions on Home Directory of the user whose umask value it is going to add/change.

Echo and Grep Commands

"ECHO" and "GREP" commands no longer required to be there in SUDOERS file. Adapter, running from SUDO/Super user account, no longer needs sudo access on these commands.

Setup for Non-English Locals

Following connector parameter has been added in the posix adapter for the enhancement to support characters from LOCALE other than English.

erposixencoding -> Code Page to be used for data encoding

The following section should be added to install guide Chapter 4. Configuring the adapter

Steps to apply the different LOCALE other than English:
1. Open DESIGN FORMS feature of the ITIM server (Under Configure System -> Design Forms)
2. Click on the Service and choose POSIX Solaris Profile. Add the attribute "erposixencoding" on the Service form from the "Attribute List" and save the form and close Design Form window.
3. Create a service with following parameters:
(refer to release notes where new parm has been added to service form)

Code Page to be used for data encoding(Default to UTF-8) : Code page to be used for data

Encoding in adapter

Set the parameter "Code Page to be used for data encoding (Default to UTF-8)" on the service form to the Code Page that corresponds to the LOCALE you are using. Like for German LOCALE the Code Page to be used is ISO-8859-1. Following is an example for the LOCALE code for German and its corresponding Code Page.

Locale code		Code Page
de_DE.ISO8859-1	or de_DE	ISO-8859-1

Setup of Key-based Authentication

The Following steps need to be added in the install guide for the DSA Key-Based authentication under section: Appendix D. Key-based authentication for the UNIX and Linux Adapter

To enable key based authentication on workstation using a UNIX or Linux operating system, perform the following on resource to be managed.

1. Use the ssh-keygen tool to create a key pair.
   a. To start the ssh-keygen tool, issue the command:
   [root@ps2372 root]# ssh-keygen -t dsa

   b. At the following prompt accept the default or enter the file path where you want to save the key pair and press Enter.
      Generating public/private dsa key pair.
      Enter file in which to save the key (/root/.ssh/id_dsa):
   c. At the following prompt accept the default or enter the passphrase and press Enter.
      Enter passphrase (empty for no passphrase):passphrase
   d. At the following prompt confirm your passphrase selection and press Enter.
      Enter same passphrase again: passphrase
      This is a sample of the system response:

      Your identification has been saved in /root/.ssh/id_dsa.
      Your public key has been saved in /root/.ssh/id_dsa.pub.
      The key fingerprint is:
      9e:6c:0e:e3:d9:4f:37:f1:dd:34:fc:20:36:67:b2:94 root@ps2372.persistent.co.in

2. Validate that the keys were generated.
   a. Issue the commands:
   [root@ps2372 root]# cd root/.ssh
   [root@ps2372 .ssh]# ls –l

   A sample system response is:
   -rwxr-xr-x 1 root root 736 Dec 20 14:33 id_dsa
   -rw-r--r-- 1 root root 618 Dec 20 14:33 id_dsa.pub
   b. Issue the command:
   [root@ps2372 .ssh]# cat id_dsa
   A sample system response is:
   -----BEGIN DSA PRIVATE KEY-----
   Proc-Type: 4,ENCRYPTED
   DEK-Info: DES-EDE3-CBC,32242D3525AEDC64

   MOZ0m/BCLFNS+ujlcnQR3gOIb5w5hwu1jByw8/kyvTMIHqAx1ANgqV1gFBGX7F0vdfmNQKnjLcH8cGueUYnmx4vSu9Fn
   KK91abNW9Nd67MDtJEztHckahXDYy7oX1tLNh3QtaZ32AgHro7QxxCGIHQeDaiGePg7WhVqH87EEXo3c+/L/5sQpfx0e
   G30nrDjl+cmXgmzU2uQsPL2ckP9NQTgRU4QgWYDBle0YhUXTAG8eW9XG9iCm9iFO4WLWtWd24Q799A1w6UJReHK
   Qq+vdrN76PgK32NMNmindOqzKVzFL4TsjLyGyWofImpG65oOFSc4GXTsRkZ0OQxixakpKShRpJ5pW6V1PN4tR/RCRW
   mpW/yZTr4qtQzcw+AY6ONAQEVtJQeN69LJncuy9MY/K2F7hn5lCYy/TOnM1OOD6/a1R6U4xoH6qkasLGchiTIP/NIfrITQ
   ho49I7cIJ9HmW54Bmeqh2U9WiSD4aSyxL1Mm6vGoc81U2XjJmcUmQ9XHmhxR4iWaATaz6RTsxBksNhn7jVx34DDvRD
   J4MSjLaNpjnvAdYTM7YislsBulDTr8NfZF6P9Fa7VyFP4TyCjUM1w==
   -----END DSA PRIVATE KEY-----

   c. Issue the command:
   [root@ps2372 .ssh]# cat id_dsa.pub
   A sample system response is:
      ssh-dss
   AAAAB3NzaC1kc3MAAACBAIHozHi6CHwvGDt7uEYkEmn4STOj2neOo5mPOZFpBjsKzzWBqBuAxoMwMgHy3zZAIgmz

MwIVQum4/uIHlhOx0Q4QDLJbveFShuXxBjm5BOU1rCCSeqYCOPdub9hx3uzZaTNqfFIvO4/NTcjp7pgQqBdvWs0loyYVi
YVWpVQmMdifAAAAFQDhaD9m//n07C+R+X46g5iTYFA9/QAAAIBVbBXXL3/+cHfbyKgCCe2CqjRESQi2nwiCPwyVzzwf
Hw4MyoYe5Nk8sfTiweY8Lus7YXXUZCPbnCMkashsbFVO9w/q3xmbrKfBTS+QOjs6nebftnxwk/RrwPmb9MS/kdWMEigd
Coum9MmyJlOw5fwGlP1ufVHn+v9uTKWpPgr0egAAAIArKV4Yr3mFciTbzcGCicW+axekoCKq520Y68mQ1xrI4HJVnTOb
6J1SqvyK68eC2I5lo1kJ6aUixJt/D3d/GHnA+i5McbJgLsNuiDsRI3Q6v3ygKeQaPtgITKS7UY4S0FBQlw9q7qjHVphSOPvo2
VUHkG6hYiyaLvLrXJo7JPk6tQ== root@ps2372.persistent.co.in

3. To enable key-based authentication in the /etc/ssh directory on the SSH server (managed resource):
   a. Ensure that the following lines exist in the sshd_config file:
      # Should we allow Identity (SSH version 1) authentication?
      RSAAuthentication yes
      # Should we allow Pubkey (SSH version 2) authentication?
      PubkeyAuthentication yes
      # Where do we look for authorized public keys?
      # If it doesn't start with a slash, then it is
      # relative to the user's home directory
      AuthorizedKeysFile .ssh/authorized_keys
   b. Restart the SSH server.

4. Copy dsa.pub to the SSH server (managed resource).
   To add the public key to the authorized keys file, from the /.ssh directory issue the command:
      [root@ps2372 .ssh]# cat id_dsa.pub >> authorized_keys
   Note: This command concatenates the DSA Pubkey to the authorized_keys file ($HOME/.ssh/ authorized_keys). If this file does not already exist, the command creates it.

5. Copy the private key file (id_dsa) to the client workstation and set its ownership value to 755.

IMPORTANT NOTE:
This adapter version does not support multiple dispatcher instances on single machine. POSIX adapter installer install the dispatcher along with connector. However multiple dispatcher instance support feature is not supported in this release as We are planning to ship all adapters from ISMP to Install Anywhere(IA).

Terminating a user session when the user is suspended

Steps to apply to kill active user process on suspending a request:

1. Open DESIGN FORMS feature of the ITIM server (Under Configure System -> Design Forms)

2. Click on the Service and choose any POSIX Profile. Add the attribute "erposixKillUserProcess" on the Service form from the "Attribute List" and also select checkbox for erposixKilUserProcess, than save the form and close Design Form window.

3. Create a service with following parameters:

   "Kill active user process on suspending an account"

NOTES:
1) "Kill active user process on suspending an account" must not be used on systems that allow duplicate user IDs.

2) 2) If any user try to suspend itself, and if the check box "Kill active user process on suspending an account" is selected, then adapter will hang.

Configuration Notes

NOTE: In Chapter 3: Configuring the UnixLinux Adapter, Section: Configuration properties of the adapter, the following properties are listed in error. These properties do not exist and they will be removed from the Installation Guide in the next release.

MaximumConnectorsPerResource	(itim_listener.properties)
ConnectorSleepTimeOut	(itim_listener.properties)
ReaperThreadTimeOut	(itim_listener.properties)

Permissions on the Tmp Folder

The file permissions on the /tmp folder must be set to 777 permission when performing reconciliation using sudo user.

Using Unix/Linux Adapter with Identity Manager Express

If using the connector with Identity Manager Express, the following entry must be made in the global.properties file before running the adapter installation.

ADAPTER_SOLDIR=TDI_HOME\soldir

Enhance the adapter to bypass invalid password file entries.

The adapter can detect and bypass some errors in the /etc/passwd file. However the fix can identify only certain type of bad records. The behavior may be different from OS to OS. User lookup commands differ for different OSes.

On Solaris

- If the shell is missing but there is a colon after the homedir then the adapter is able to handle this and treats shell as blank and recon is successful
- If the shell is missing and there is no colon after the homedir then the logins command itself fails which is identified as a bad entry and recon continues with error msg in log file

On Linux

- If the shell is missing but there is a colon after the homedir then the adapter is able to handle this and treats shell as blank and recon is successful
- If the shell is missing and there is no colon after the homedir - No command is used on Linux, the /etc/passwd record for this user is read and parsed based on colons. In this case the data is misinterpreted and recon fails.

In general it must be noted that:

- the UnixLinux recon depends heavily on the structure of /etc/passwd and /etc/shadow to be correct - especially for Linux and Solaris.
- Even though some bad entries may be identified it may not be possible to identify all types of bad entries.

New Adapter Features

Log Warning for Unsupported OS Versions

The adapter has been enhanced to tolerate unsupported OS versions and distributions. No configuration is required for this feature. If the adapter detects an unsupported version, it will log a warning message in ibmdi.log for unsupported OS and continue with the requested operation if possible. For example, if your Linux distribution is a variant of RHEL, the adapter may operate correctly. Note that you may also need to configure the password prompt (see Externalized Password Prompt Strings).

Externalized Password Prompt Strings

The Unix/Linux Adapter performs password changes using an interactive SSH session. The adapter must know the expected password prompt to complete the transaction successfully. To enhance the flexibility of the adapter, this password prompt is now configurable by Service.

To enter your own password prompt regular expression, follow these steps.

Step 1: Add the Password Prompt attributes to the Service Form using the TIM UI form customization tools:

a) From the “Configuration” tab select “Form Customization”. Expand the “Service” option on the left pane and select the proper service profile (POSIX AIX profile, POSIX HP-UX profile, POSIX Linux profile, or POSIX Solaris profile).
b) From the “Attribute List”, add the following two attributes to the form: “erPosixNewRegx” and “erPosixRetypeRegx”.
c) Click on save options on top of form to save this attribute on service form.
d) Note: These changes will be reflected on all service forms of this service type (profile).

Step 2: Enter the desired password prompt regular expression:

a) From “Service Management”, select the service in question and update the service form by adding regular expressions to the newly added attributes.

Example Password prompt for your OS is "Enter new Password:"
Enter the regular expression as ".* Password:".

Retype password prompt for your OS is "Reenter new password:"
Enter te regular expression as "Re.* Password:" or ".* Password:".

Where “.” (period) represents any character and “*” represents one or more occurrences of the character.

Support for Pre/Post Exec Attributes

The Pre/Post Exec attributes have been added to the default adapter schema to ease the configuration of these features. Due to the sensitive security requirements of this feature, the attributes are not on the default account form.

To add support for PreExec, PostExec attributes follow these steps

1) From the “Configuration” tab select “Form Customization”. Expand the “Account” option on the left pane and select the proper account profile (POSIX AIX account, POSIX HP-UX account, POSIX Linux account, or POSIX Solaris account).

2) From the “Attribute List”, add the following two attributes to the form: “erposixpreexec” and “erposixpostexec”.

3) Click on save options on top of form to save this attribute on account form.

4) Note: These changes will be reflected on all account forms of this service type (profile).

Adding home directory permission on the account form

The home directory permissions can be added to the account by using the “Form Customization" in the TIM UI. Add attribute erPosixPerHomeDir with a "umask" widget to any of the UNIX/Linux account forms.

AIX 6.1 Roles Support

For version Aix 6.1 and above the lsrole command is used. If using version aix 6.1 or higher add the command /usr/sbin/lsrole in sudoers file:
eg -

tdiuser ALL=NOPASSWD:/usr/sbin/lsrole,/usr/bin/sed,/usr/bin/pwdadm, /usr/bin/passwd,/usr/bin/mkuser,/usr/sbin/rmuser,/usr/bin/chuser,/usr/bin/chmod,/usr/bin/cat,/usr/bin/echo,/usr/bin/grep,/usr/bin/rm,/usr/bin/rmuser,/usr/bin/tee,/usr/bin/ed, /usr/bin/groups, /usr/bin/ls,/usr/bin/logins,/usr/sbin/lsuser

NOTE: If there is prior version Aix 6.1 service then it may have incorrect roles (IZ30567 - PMR 56327,999,866). Delete the old service, create a new one and run a fresh recon. If not able to delete the service then delete all roles from LDAP manually or create a new service.

Disable Caching Feature

Steps to use the new feature - Diable AL caching for a particular service

1. Go to form customization tab on configuration menu for 46 ITIM and design form for 50 ITIM. Double click on service and select appropriate service for which you want to disable the AL caching.
2. On right side there is attributes list that you can add on service form.
3. Double click on ‘erposixdisablealcache’ attribute from attribute list, this attribute will get added on service form.
4. Mark the attribute type as check box default it is textbox.
5. There is one button on service form to save the changes, click on that button to save the changes.
6. Open service form again and see ‘Disabled Al Caching’ new check box attribute will get added on service form.
7. By default the check box is off so Al caching is on for newly created service.
8. Make check box on to disabled the AL caching for this service only.
9. After making this check box on, test/add/mod/del AL will not cache in cache array.

RXA Timeout Feature

There are 2 types of end resource commands that come into picture for POSIX connector:
a. Commands which are fired by connector using RXA library.
b. Commands which are internally fired by RXA library against RXA APIs
(ex during Connection establishment, during Resource version detection). Example provided below.

This enhancement is related to type (b), the commands which are internally by RXA library, as a result of some RXA API getting invoked from connector. The problem occurs when commands internally fired by RXA library take more than default time to execute. In this case, API fails with timeout error. RXA library provide a method to set the timeout for these internal commands , in such scenario , so that command will return success.

In order to configure that timeout, a new property is added on Service form of Adapter named "RXA Internal Command TimeOut". It accepts value in terms of milliseconds. If not set, RXA will use default value for internal command timeout, which is 5000 ms by default. If it is set, then RXA will use specified value for internal command timeout. This property should be set only in the case mentioned above, where end resource take more time to execute internal commands fired by RXA.

NOTE: There is one more property associated with RXA. It is Session timeout property. This has a relation with internal timeout property. The default value of "RXA Internal Command TimeOut" is 5000 ms and default value of RXA Session timeout is 30000 ms. If customer set "RXA Internal Command TimeOut" value on service form, up to 30000 ms, then session time out will remain to its default value 30000 ms. But if the "RXA Internal Command TimeOut" on the service form is more than 30000 ms (say 50000 ms), then the same value will be set to Session timeout value by connector. Connector needs to do it, because if session timeout is less than "RXA Internal Command TimeOut", the "RXA Internal Command TimeOut" will not have its effect, and session timeout will take a preference.

User Private Group Control

A new option has been added to control the creation of User Private Groups on Linux. A new attribute "Do Not Create User Private Group" is added on the account form.

"Do Not Create User Private Group" provides an option to customer not to create a private group every time a user account is added on the Linux resource. If customer will select the option "Do Not Create User Private Group", no private group will get created on the resource for that user. By default, Linux Redhat creates a private group for each user.

Note: "Do Not Create User Private Group" option is only supported on Redhat Linux not on SUSE, as SUSE does not support/create a private group for each user.

Home Directory Processing Enhancements

This version of the POSIX adapter is enhance to create a default Home Directory for a user/account on Linux, Solaris and HP-UX systems. The adapter will provide an option for user to select to create a Default Home Directory for an account. The Default Home Directory will be created by concatenating the BASE DIRECTORY (Base Directory value that is defined on that system) with the AccountName/USERNAME to be created.

Example: Suppose on the target system, BASE DIRECTORY's value is "/home" and the username for the account that is being created is "testuser", then Default Home Directory that will get created will be with name "/home/testuser".

Note: This enhancement is for all the OS except AIX, as AIX systems by default create a Default Home Directory for each newly created account. So its effect will be for Linux, Solaris and HP-UX systems only.

Specifying the Location of the Adapter Scripts

This version of the POSIX adapter will provide an option for the users to change the default location where the adapter script will get copied. User can enter any desirable path on the target/managed system where adapter scripts should be copied.

Note: This option is per service configurable. By default, this option will not be there on Service Form. However, user can choose this option from DESIGN FORMS of IBM Tivoli Identity Manager (ITIM) server.

The attribute that will be representing this option is named as "erposixcopyadpfilesto". The default value for this attribute is "/tmp" folder on the target system. However, user can change it to any valid path/location on the target system.The user which is been used as an Admin user on the ITIM service form should have enough permission on the location/directory specified as a value for this option.

Status from Pre-Post exec script execution.

This version of the POSIX adapter is enhance to provide an option to decide whether to continue with the operation depending on the status of Pre-Exec and Post-Exec commands. Following options will be available:

for each account (On Account Form):

Pre Exec Options:
- Always execute operation
- Execute operation only when Pre-Execution command succeeds

Post Exec Options:
- Always execute Post-Execution command
- Execute Post-Execution command only when operation succeeds

Under Pre Exec Options,
- -> The first option, "Always execute operation", means continue with the actual User Provisioning Operation irrespective of the status of Pre-Exec command.
- -> The second option, "Execute operation only when Pre-Execution command succeeds", means continue with the actual User Provisioning Operation only if Pre-Exec command succeeds.

Under Post Exec Options,
- -> The first option, "Always execute Post-Execution command", means execute Post-Exec command irrespective of the status of User Provisioning Operation.
- -> The second option, "Execute Post-Execution command only when operation succeeds", execute Post-Exec command only if User Provisioning Operation succeeds.

Note: User Provisioning Operation means any of the account management operations like User Add, User Modify etc. The status of Pre-Exec and Post-Exec commands will not get returned to ITIM server.

In Modify request, ITIM server will not send values for Pre-Exec and Post-Exec until their values have been modified. If users wants to send values for Pre-Exec and Post-Exec in each Modify operation, then

they can put following statements in service.def file for that particular profile. Following are the exact steps to modify the service.def file to send the value of Pre-Exec and Post-Exec in modify request.

a. Un-jar the Profile.jar, e.g. PosixAIXProfile.jar.
b. Open Service.def file in some Text Editor.
c. Put following lines in the Service.def, under <operation cn="posixModify">

```
<input name="erPosixPreExec" source="erPosixPreExec"></input>
<input name="erPosixPostExec" source="erPosixPostExec"></input>

<input name="erPosixPreExecRunOption" source="erPosixPreExecRunOption"></input>

<input name="erPosixPostExecRunOption"
source="erPosixPostExecRunOption"></input>
```

d. Save the changes and create Profile.jar, e.g. PosixAIXProfile.jar using following command:
Jar -cvf PosixAixProfile.jar PosixAixProfile

Using "hostsallowedlogin" and "hostsdeniedlogin" Attributes

This version of the POSIX adapter is enhanced to support two new AIX attributes, named “hostsallowedlogin" and "hostsdeniedlogin". Please refer to AIX documentation for more details on these attributes.

A few characters are not valid to be used in the value of "hostsallowedlogin" and "hostsdeniedlogin" so ITIM server will not allow to submit a request if any of these characters are there in the value of these attributes as there is a constraint that is put on user account form. The list of the characters which are not allowed contains `!&()|;'"

Some of the above characters are allowed as valid but these have special meaning on AIX systems so adapter is having a constraint on them. However, users can customize the list of invalid characters as per their setup using DESIGN FORMS on ITIM Server.

Note: This version of the adapter expects the values of these attributes in REPLACE form (Instead of Add/Delete form) while modify request. ITIM server v4.6 should have appropriate FIX Pack applied to send the values in REPLACE form.

Support for Other Linux Distributions

For Linux systems, adapter behavior has been changed to take the default as REDHAT, if no appropriate Release file is present in /etc folder. Adapter will dump a log message ("This Linux OS version may not be supported") and proceed.

Note: This change has been made for Linux OS only.

APAR IZ76603 - Path to faillog used by ITIM adapter

PMR-15219,999,000 - Path to faillog used by ITIM adapter in release notes should be updated. Updates to Install Guide:The path given in install guide for sudo may vary from resource to resource. The sudo command path given in install guide or release note is an example. The actual command path on resource might be diffrent, so user need to add correct path of the command into sudoers file.

APAR IZ75546 - at.allow/at.deny/cron.allow/cron.deny corruption

IZ75546 ,PMR 31640,004,000 - at.allow/at.deny/cron.allow/cron.deny corruption when deleting accounts.

Adapter creating lock directory "POSIXLCK" into /tmp folder before editing at and cron files. If user has specified different tmp directory name on service form then adapter will create lock directory into user specified directory.

Please make sure that POSIXLCK folder does not exist inside /tmp or user specified temp directory. If this directory is allready exist, then adapter will fail to set at and cron attribute values.

APAR IZ73366 - UNIXPOSIX ADAPTER 5.0.11 FAILS RECONCILING GROUP-ID ON AIX-LDAP

Tivoli PMR 94202,100,838. Earlier version of adapter fails to recon group information if Aix is configured with LDAP server. The adapter is enhanced to recon group data from Aix-LDAP setup.

Note - If Aix is configured with LDAP server then adapter return group data from LDAP server as well as /etc/group file.

Double Quotes in Home Directory

Earlier version of adapter returns failure on HPUX, if home directory value contains double quotes. But resource added the account without a home directory.

The fix is also provided for other platforms and fix details are as below

Aix : The fix is provided to modify homedirectory Permissions, umask and delete an account, if homedirectory contains double quotes.

Solaris : The fix is provided to modify homedirectory Permissions, umask and delete an account, if homedirectory contains double quotes.

Linux.: The fix is provided to modify homedirectory Permissions and umask , if homedirectory contains double quotes.

Note:- On HPUX, As resource does not allow to create home directory with double quotes,from this release ITIM will not send value of home directory with double quotes.

Group Names with "()"

Earlier version of adapter was getting hang when a group with have () is assocaited with user in useradd request. The fix is provided on Aix, such that it will add or modify an account if group contains (). The fix is also provided for AUTH1, AUTH2 attribute, It will allow () for AUTH1 and AUTH2 variable.

Note : The fix is provided for multi-value attribute, but single value attribute might need a fix.

Transaction Status on Suspending Suspended Accounts

The earlier version of adapter returns failure on HPUX-Nontrusted on suspending a suspended account and restoring an active user.

The fix is provided so it will return warning on suspending a suspended user and restoring an active user.

Account Status on Recon

Earlier version of adapter reconcile account as active even if it is suspended. The fix is provided so that it will return suspended account as suspended and active account as active for Linux NonShadow.

Home directories containing a Space character

The earlier version of the adapter could not set the umask value in the profile file, could not modify homedirectory permissions and could not delete home directory, if home directory contains space. The fix is provided to set umask value, to modify homedirectory permissions and to delete homedirectory, If homedirectory contains space.

Terminating a user session on suspend

UnixLinux adapter is enhanced to optionally terminate user session when user is suspended. This version of Posix adapter is enhance to provide an option to decide whether to kill all active process of user on suspending a user or not.

Behavior: After suspend request executed successfully, the active processes for that user get killed. This is optional. If you don't select check box "Kill active user process on suspending an account", it will not kill user processes.

NOTE: The ADK based adapter kills the active user process before suspending a user, but TDI based adapter will kill after suspending a user, the reason is if suspend request fails then it should not terminate user processes.

Prerequisites: On Hpux, we support this enhancement if any only if output of ps -u username is in following format, i.e. PID should be in 1st column

```
PID TTY      TIME COMMAND
10702 ?       0:00 sshd
10704 pts/1   0:00 sh
```

On Other resources, we support if and only if the name of column pid remains pid.

Whenever the value of the checkbox "Kill active user process on suspending an account" is changed, the Dispatcher must be restarted.

NOTE: "Kill active user process on suspending an account" must not be used on systems that allow duplicate user IDs. If the user of a duplicate ID tries to suspend his account, and if the check box "Kill active user process on suspending an account" is selected, then adapter will hang.

NOTES:

3) "Kill active user process on suspending an account" must not be used on systems that allow duplicate user IDs.

4) 2) If any user try to suspend itself, and if the check box "Kill active user process on suspending an account" is selected, then adapter will hang.

Adapter Troubleshooting Guide

The following information may be helpful to troubleshoot adapter installation and operational problems.

Note that the following steps are written for the AIX platform and should be updated with proper commands for other UNIX/Linux platforms.

The term "adapter username" is used throughout this procedure. The "adapter username" is the UNIX account supplied on the TIM service form for the administrator name. This is the account used by the adapter to open a connection to the target machine.

1) Set log level to debug max (refer to installation guide). If possible, get the log file with the failed request only.

2) Get software versions:

   a. Dispatcher version: log file search string (RMIDispatcherImpl: Starting)
   b. Assembly line version: logfile search string (UNIX/Linux Adapter AL version)
   c. Posix Connector version: logfile search string (Loaded com.ibm.di.connector.osconnector.PosixConnector)
   d. RXA library version: logfile search string (RXA Version)

3) Get OS version. On the AIX machine, issue the following commands:

   % instfix -i | grep AIX_ML
   % oslevel -q –s

4) Make sure that "sh" is the default shell for the "adapter username".

5) Make sure OpenSSH is used. OpenSSH is the only supported ssh package. No other ssh vendors are supported.

   Get OpenSSH version: on AIX, issue the following command:

   $ ssh –version

   AIX note: although other versions of OpenSSH function properly with this adapter, the AIX development team requires that OpenSSH version 4.7 or higher should be installed. You may be required to update your OpenSSH version to get support if the issue is traced to OpenSSH.

6) SSH Configuration:

   UsePrivilegeSeparation must be set to yes in the sshd_config file otherwise the adapter account will be locked. The defaults value of UsePrivilegeSeparation is yes.

7) From the command line, on a remote machine, issue the following "ssh" commands and capture the results.

   % ssh username@ip-address "ssh -version"

   if sudo is used:

   % ssh username@ip-address "sudo ls /tmp"
   % ssh username@ip-address "which sudo"

   where: username is the "adapter username".
   ip-address of the AIX machine being managed.

8) If a recon issue:

   - Copy file AIXPConnRes.sh recon file the adapter solution directory to the AIX /tmp directory.
   - Login to the AIX machine with the "adapter username".
   - Change directory to /tmp
   - Make sure you have execute permission on AIXPConnRes.sh (chmod 777 AIXPConnRes.sh).
   - Run the following command and save the recon.out file:

   AIXPConnRes.sh "grep -e :" true > recon.out 2>&1 (note: if sudo is not used, replace true with false).

   Note: other platforms recon files are (all files are located in the adapter solution directory):

AIX file system:	AIXPConnRes.sh
AIX LDAP:	AIXPLDAPConnRes.sh
HPUX not trusted:	HPNTrustPConnRes.sh
HPUX trusted:	HPTrustPConnRes.sh
Linux (no shadow):	LinuxPConnRes.sh
Linux (with shadow):	LinuxShadowPConnRes.sh
Solaris:	SolarisPConnRes.sh

9) Make sure TDI FP0003 or higher have been installed on TDI 6.1.1.

10) If sudo is used:

    - Verify sudo setup per installation guide.
    - Login to the target system using the "adapter username".
    - Perform manual commands using sudo on the target machine:
      For example:
      - sudo mkuser test1
      - sudo passwd test1
      - sudo rmuser test1
    - Get a copy of sudoers file or at least a section of the file that shows the "adapter username" entry.

Updates to the Troubleshooting Guide

Trouble shooting additions for Chapter 6

- Warning or Message: CTGIMT022E The search failed due to a system error: Error executing script with Failed value : 126

  Recommended action: Verify the TDI 6.1.1 Fix Pack 3 is installed. Verify the sudo user configuration file does not contain syntax errors.

Update the section Appendix C : Creating a super user on a supported operating system

- Under section - Creating a super user on an AIX operating system, add following step:

  2.c. To validate the format of /etc/sudoers file, issue the following command: "visudo -c". This command will verify the syntax of /etc/sudoers file. If syntax is wrong it will prompt an error message, e.g.

  $ visudo -c
  >>> sudoers file: syntax error, line 30 <<<
  parse error in /etc/sudoers near line 30

Under section - Creating a super user on a Linux operating system

- Add following step:

  2.c. To validate the format of /etc/sudoers file, issue the following command: "visudo -c". This command will verify the syntax of /etc/sudoers file. If syntax is wrong it will prompt an error message as mentioned above.

Under section - Creating a super user on a Solaris operating system

- Add following step:

  2.c. To validate the format of /etc/sudoers file, issue the following command: "visudo –c". This command will verify the syntax of /etc/sudoers file. If syntax is wrong it will prompt an error message as mentioned above.

Under section - Creating a super user on a HP-UX NonTrusted operating system

- Add following step:

  2.c. To validate the format of /etc/sudoers file, issue the following command: "visudo -c". This command will verify the syntax of /etc/sudoers file. If syntax is wrong it will prompt an error message as mentioned above.

Under section - Creating a super user on a HP-UX Trusted operating system

- Add following step:

  2.c. To validate the format of /etc/sudoers file, issue the following command: "visudo -c". This command will verify the syntax of /etc/sudoers file. If syntax is wrong it will prompt an error message as mentioned above.

  NOTE: If you get an error messge like "visudo: not found." while running "visudo -c". Locate the exact path of "visudo" command, using "find / -name visudo" command and then use the complete/absolute path of "visudo" command, e.g. "/usr/local/sbin/visudo -c"

Supported Configurations

Installation Platform

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

Adapter Installation Platform:

This adapter installs into Tivoli Directory Integrator (TDI) and may be installed on any platform supported by the TDI product. IBM recommends installing TDI on each node of the ITIM WAS Cluster and then installing this adapter on each instance of TDI. Supported TDI versions include:

TDI 6.0 is no longer supported.
TDI 6.1 is no longer supported.
TDI 6.1.1 with Fix Pack3 (or later)

NOTE: Many of the closed APARs in this adapter rely on fixes in TDI v6.1.1 FP3. Fix Pack 3 (or later) is a prerequisite for this version of the adapter.

Managed Resource:

AIX

AIX 5.1, 5.2, 5.3, 6.1

Solaris

Solaris 8, 9, 10

HP-UX

HP-UX 11i	(trusted, non-secure)
HP-UX 11i	(non-trusted)
HP-UX 11i v2	(trusted, non-secure)
HP-UX 11i v2	(non-trusted)
HP-UX 11i v3	(trusted, non-secure)
HP-UX 11i v3	(non-trusted)

SuSE Enterprise Linux Server (SLES)

SLES 8, 9, 10, 11

RedHat Enterprise Linux (RHEL)

RHEL AS 3.0, 4.0, 5.0
RHEL ES 3.0, 4.0, 5.0

Debian

Debian Linux 5.0.2

IBM Tivoli Identity Manager:

ITIM Express	v4.6.0
ITIM Enterprise	v4.6.0 with FixPack 4.6.0-TIV-TIM-IF0085

IMPORTANT NOTE:

This Adapter does not support NIS, or NIS+. Please use available agent-based Adapters for this purpose. LDAP registry is supported only on AIX.

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