Axel Buecker
David Edwards

Tivoli Identity Manager and Reverse Password Synch Modules

Introduction/Overview

This document describes how the IBM® Tivoli® Identity Manager reverse password synchronization mechanism works. This mechanism is used by most clients as a vital component of their Identity Manager deployment, but there are areas where this mechanism could be better documented. This paper aims to provide a comprehensive technical guide to this key component of Identity Manager.

This document focuses on the Windows® Reverse Password Synch modules, because they are deployed most often. However, it also describes the other modules and the password synchronization provided through IBM Tivoli Directory Integrator.

Thanks to Masa Imokawa, Jason Wu, Rob Schey, and Subbu Cherukuwada for providing input and review of this document.

Overview of Identity Manager and password synchronization

This section introduces the password synchronization feature of Identity Manager.

Password synchronization

Identity Manager does not provide a single-signon capability; it provides a “reduced” signon by allowing all passwords for a user’s accounts to be synchronized so a user only needs to remember a single password.

This is driven from Identity Manager (the Identity Manager server) down to all of the target systems based on a change made by the user or administrator. Identity Manager associates all accounts with a person object, so one password change can be applied to all of the accounts for a user. Also, password policy (the strength and history rules) is applied to people, so that different sets of users can have different policies applied to all of their accounts (for example, administrators might have a tighter policy than ordinary users).

This is the normal password synchronization provided by Identity Manager.

The challenge with this approach is that there is no way to force a user to go into Identity Manager to change their password. You can encourage users to periodically log in and change their password; you can even put a link on the front page of the intranet, but you still get users whose LAN passwords expire, and they change them when prompted, which means their account passwords are out of synch. This is where reverse password synchronization comes into play.

Reverse password synchronization

Reverse password synchronization is where a password change on one of the target systems, such as in a Windows Domain Controller or WebSEAL, is used to synchronize all of the other account passwords for that user.

This solves the problem of users relying on the system to prompt them to change their passwords. Most environments have a limited number of entry points, such as a LAN login or a Web-based login (such as logging into a portal or intranet). The reverse password mechanisms hook into the existing password management mechanisms and synchronize the passwords without the user being aware of it.

If you have deployed a single-signon (SSO) solution, the password synchronization and reverse password synchronization mechanisms can distribute the new password to the SSO account repository in the same way that it does for other targets.

The Identity Manager reverse password synch mechanism

The Identity Manager reverse password synch mechanism performs two functions: password policy enforcement (that is, strength and history checking) and password synchronization (keeping all account passwords the same for a user). You can enable both of these functions, one only, or none of them.

The flow of the reverse password synch mechanism is shown in Figure 1 on page 3.

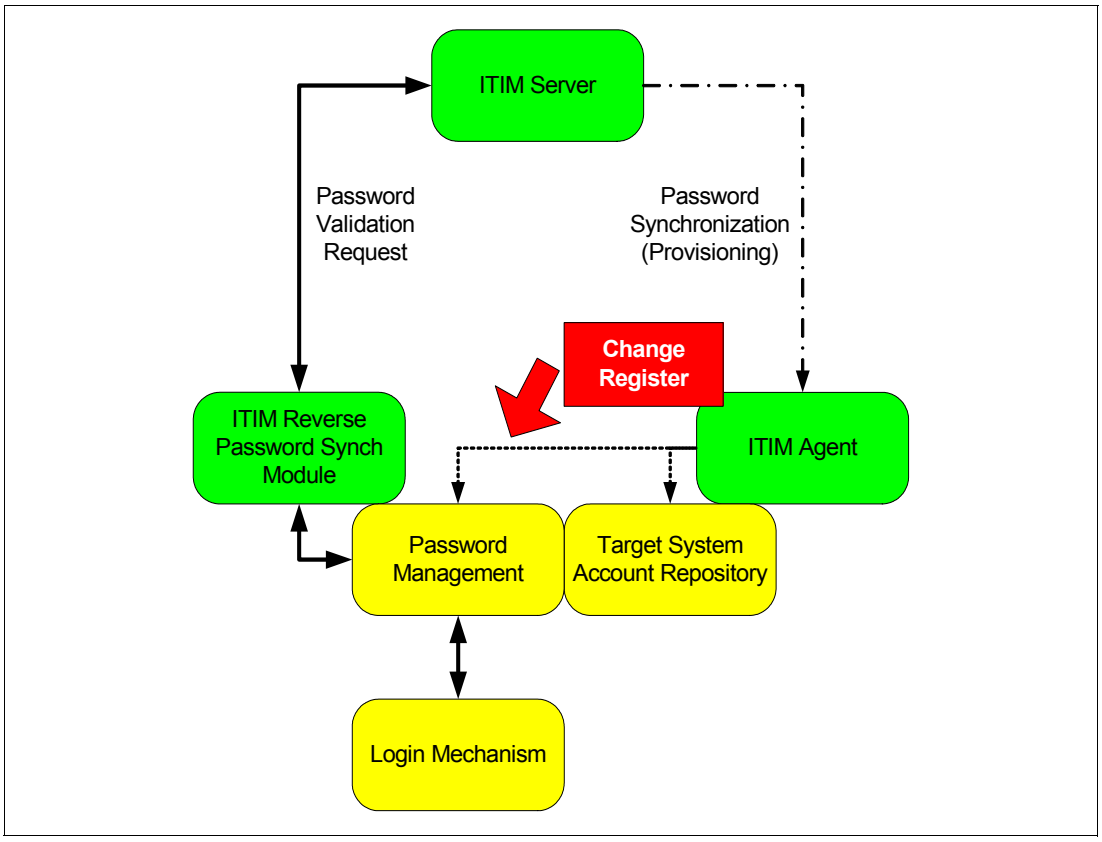

Figure 1 Reverse password synch mechanism flow

The user logs in and receives a prompt to change the password from the native login mechanism (such as the Windows login mechanism). The Identity Manager module is hooked into this native mechanism so that the Identity Manager module can capture the new password in the clear before the new password is encrypted or hashed. This new password, along with the user ID, is passed up to the Identity Manager server.

If policy checking is enabled, the new password is checked for compliance and a success/reject response is sent back to the module. If password synchronization is enabled, the passwords for all other accounts owned by this user are set to the new password, and provisioned out to the target systems through their provisioning adapter (that is, the Identity Manager adapter).

These steps are described in more detail in the following sections.

Capturing the password in the clear

The first step in the reverse password mechanism is capturing the newly set password. This must be done prior to the new password being encrypted or hashed. Identity Manager does not replace the existing native login mechanisms; it hooks into the existing mechanism using whatever means is provided.

For example, Windows provides the Local Security Authority mechanism that allows additional password mechanisms to be hooked into the password change loop.

Contacting the Identity Manager server

When the reverse password synch module is called, it determines the location of the Identity Manager server (Web address of the host and the port) and the domain name (DN) of the service that relates to this reverse password synch module from its configuration. The reverse password synch module calls the Identity Manager server's password synch servlet using HTTPS with a Web address, such as https://<*server host*>:<*port*>/passwordsynch/synch.

Note that this is the same server and port Web site that the normal (browser) UI accesses. If a High Availability (HA) or high performance Identity Manager solution is in use with browser access load-balanced through a front-end load balancer, the password synchronization requests are also load balanced across multiple Identity Manager cluster nodes.

The Identity Manager server will be called if either the password synchronization or policy enforcement functions are enabled. The reverse password synch module must have an account to log into Identity Manager (called the Identity Manager principal).

The account ID, new password, and service DN are passed to the Identity Manager server. The synch servlet uses this information to determine the person object for this account.

Verifying policy

If password policy checking is enabled, Identity Manager determines which password policy to apply for this service, based on the normal inheritance rules for objects in the Identity Manager Org Tree. Identity Manager checks the new password against the relevant policy and sends a response back to the reverse password synch module.

If password synchronization is enabled, it will need to consolidate the password policies for different accounts to ensure that the new password meets all policies that apply to all of the accounts. This is the same as though you change a password through the Identity Manager UI for multiple accounts where password policies are combined to enforce a single password that complies with all target system policies.

Synchronizing passwords

If password synchronization is enabled, Identity Manager generates a password change request for every account that is attached to this person. It does not generate a password change request for the service associated with the password synch module. For example, if the request has come from the Tivoli Access Manager for e-business WebSEAL password synch module, a password change request is not sent to the Access Manager for e-business adapter.

In order for password synchronization from the reverse password synch modules to work, password synchronization must also be set within the Identity Manager server (configuration setting).

Closing the loop

The provisioning adapters (that is, the normal Identity Manager adapters) use the native account mechanisms, including the password management mechanisms. So a password synchronization request that has originated from Identity Manager can result in a reverse password synch request flowing back up to Identity Manager, producing unnecessary network traffic.

To resolve this issue, the provisioning adapters associated with a reverse password synch module log password changes into a registry. The reverse password synch module reads this registry and does not send the request up to Identity Manager if the request was initiated by the provisioning adapter. The registry is a rolling log of the user name, a hash of the

password, and a time stamp. The lookup for uniqueness is the user name and password. On Windows systems, this is held in the Windows registry.

Reverse password synch modules

There are two types of reverse password synch modules: the standard Identity Manager ones that ship with the relevant provisioning adapters and the IBM Tivoli Directory Integrator password interceptor connectors.

The most common Identity Manager reverse password synch modules are the Windows ones. This section looks at each one in detail.

Windows Reverse Password Synch module

A reverse password synch module has shipped with the Windows Agents (adapters) since before IBM acquired Access360®. The current reverse password synch module only ships with the Windows AD adapter. The Windows local adapter does not ship with the module.

For example, the Windows AD adapter Version 4.6.13 ships with the 4.6.6 version of the Windows Password Synch Plug-In.

Note: Much of the information that we list for the Windows AD Reverse Password Synch module applies to the Identity Manager reverse password synch module, such as SSL configuration and architecture/policy considerations.

Sample flow of the Windows module

The following steps describe the flow when Windows prompts me (in an AD Domain) to change my password:

1. I enter my new password into the normal Windows Change Password dialog and click OK.
2. The workstation contacts a domain controller and passes the user credentials (the user ID and the new password).
3. The domain controller performs its password checks and then passes control to the Identity Manager AD reverse password synch module (and any other modules defined as Local Security Authority Notification Packages).
4. The AD reverse password synch module looks up the registry for the AD (provisioning) adapter to determine if this password change request came from Identity Manager. Because the password change request did not come from Identity Manager, processing continues.
5. The AD reverse password synch module determines my base point in AD and uses this to determine the related Identity Manager service DN (from the reverse password synch configuration).
6. The password change request is sent from the reverse password synch module to the Identity Manager passwordsynch/synch servlet.
7. This servlet performs the password policy check and sends a response back to the reverse password synch module, which returns it to Windows. If password synchronization is *not* enabled, Identity Manager only checks the policy that applies to the AD service. If passsword synchronization is enabled, it lists the accounts that I own, determines the combined password rules for all of my accounts, and checks against those rules.

8. If the password change was successful, I continue into Windows; otherwise, I get prompted for another new password.
9. If password synchronization is enabled, it also sets the new password on all of the other accounts associated with my person object (that is, all of my other accounts). This generates provisioning requests down to the systems holding these accounts using the normal Identity Manager provisioning mechanisms.

Architectural considerations

The Windows reverse password synch module must be installed on every Domain Controller in a domain, because this is where the Windows password change mechanism runs. Note that this differs from the provisioning adapter, which can be deployed to any server in the domain.

So it is possible that you will have the reverse password synch module on a different server than the provisioning adapter (a number of clients have this architecture). The two components are designed to work in this way, but you need to ensure that the appropriate remote registry rights are set up (see “Remote registry access” on page 14).

Policy considerations

There are two settings that you need to consider: password synchronization and policy enforcement (that is, *Enable Password Rules Verification*). You can enable none, password synchronization only, or both of these settings. The behavior differs in each case:

- If both are disabled, the reverse password synch module is effectively turned off. The module will be called by Windows but will not do anything.
- If only password synchronization is enabled, Identity Manager will only be used to find the other accounts for this person and send the new password to those accounts. Identity Manager will not do any policy enforcement. If the reverse password synch module cannot contact the Identity Manager server, the password change will be successful in AD, but not on the other systems (this can cause problems with SSO solutions).
- If both password synchronization and policy enforcement are enabled, the reverse password synch module will use the Identity Manager server for both synchronization and policy checking. If the Identity Manager server is not available, the password change fails in Windows. In the case of a failure, you get a generic Windows error message; the error message does not explain why the new password failed the policy.

Note that the latest version of the reverse password synch module (Version 4.6.6) has a configuration setting with policy enforcement that requires a response from the Identity Manager server (or not). So if this option is not selected, the reverse password synch module does not wait for Identity Manager to respond to a policy enforcement request.

So you need to consider how you want your password policy enforced; if passwords must always be checked by Identity Manager, you need to ensure that the Identity Manager server and the application have a high level of availability.If you are only concerned about synchronization and having passwords out of synch due to the occasional network issue, then you can disable policy enforcement (that is, rely on Windows policy checking) and only use Identity Manager for synchronization.

This is a business decision as much as it is a technical one. The business needs to decide whether they need to centrally control password strength and enforce synchronization or not.

What is installed and where it is installed

There are three parts to the reverse password synch mechanism: the reverse password synch module, the Identity Manager server code that responds to requests from the reverse

password synch module, and the AD adapter. This section looks at what is installed for each component.

The Windows Reverse Password Synch installation image

The adapter installation image (zip file) contains three files that relate to the reverse password synch module: the module installer (.exe), a text readme file, and a PDF installation guide. The text readme file contains information relating to supported platforms, new features, and fixes and code changes from different releases. The PDF installation guide describes the steps to install and configure the module.

The standard installation creates a folder named c:\Tivoli\PasswordSynch. This folder contains subfolders that contain the installation Java™ Virtual Machine, uninstall files, and two utilities:

- CertTool.exe: the tool for working with certificates for the reverse password synch module
- pfconfig.exe: the tool for changing the configuration settings (this is the utility that runs as part of the installation process)

The standard installation also installs a file TivoliPwdSync.dll into the C:\WINDOWS\system32. This is the reverse password synch module that intercepts the password change and sends the request to the Identity Manager server.

The installation also creates a registry key:

HKEY_LOCAL_MACHINE/Software/Access360/pwdsync

This key contains the configuration settings for the module, as shown in Figure 2.

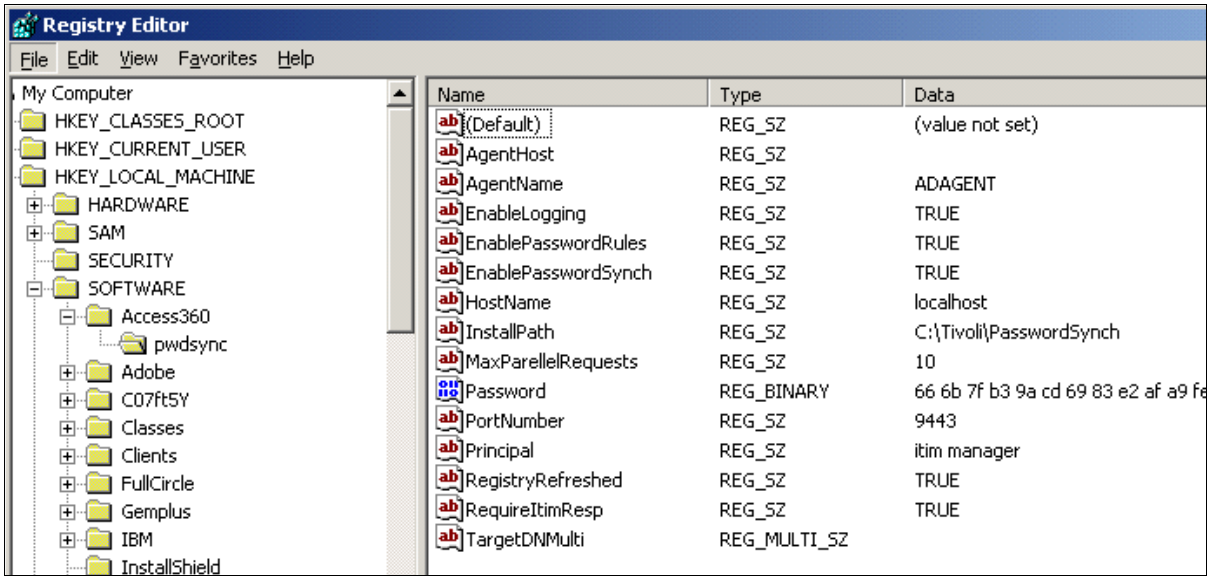

Figure 2 Configuration settings for the module

It also adds an entry to the Local Security Authority (LSA) Notification Packages registry entry (described in the next section).

The AD adapter installation image

There are no additional code or data files deployed as part of the adapter to implement the reverse password synch mechanism (the changes are embedded in the adapter code).

There is the AD adapter registry, which contains a record of the password changes initiated by Identity Manager (described in a following section).

The Identity Manager server servlet

The server-side part of the mechanism (servlet) is installed as part of the Identity Manager server. There is a war file, passwordsynch_web.war, that is installed within the enRole.ear directory (under the normal WebSphere® Application Server installedApps/<*server*> directory). The WebSphere Application Server HTTP server plug-in routes all requests from the HTTP server to WebSphere Application Server, and WebSphere Application Server uses the appropriate Identity Manager application module based on the Web address (in this case, passwordsynch/synch). There is no specific configuration file or other data files for this code.

Technical implementation details

This section contains details about several of the more technical aspects of the AD reverse password synch module.

How to implement password interception

The reverse password synch module is hooked into the Windows login mechanism through the Local Security Authority (LSA) registry key.

The HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages value lists the modules that will be processed, in order, for password change operations. This list appears in Figure 3.

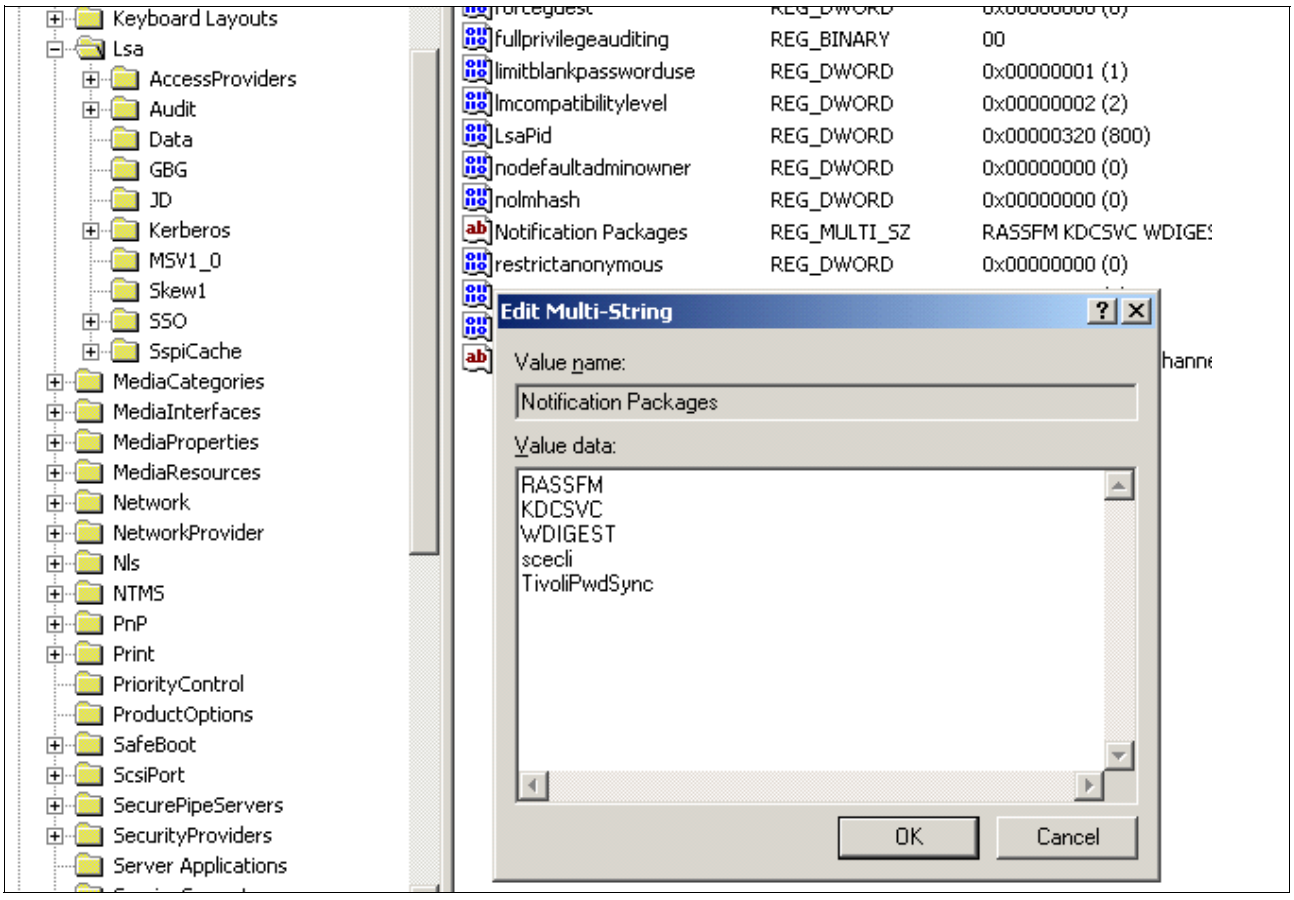

Figure 3 Modules to process for password change operations

The entries that display depend on the Windows version. Figure 3 on page 8 is for a Windows Server® 2003 server. A Windows 2000 Server system might list FPNWCLNT, RASSFM, KDCSVC, scecli, and TivoliPwdSync. If a client has deployed additional modules, the additional modules are listed here as well.

The reverse password synch installation mechanism adds the TivoliPwdSync entry to the registry key value.

For a great description about how the Windows login mechanism works (and how you can extend it), see:

http://technet2.microsoft.com/WindowsServer/en/library/779885d9-e5e9-4f27-9c14-5bbe77b056ba1033.mspx

Look at the LSA section about halfway down the page. This page is for Windows Server 2003.

You can see the details of the LSA Notification Packages registry entry (Windows Server 2003) in:

http://technet2.microsoft.com/WindowsServer/en/library/5d71e79e-cbdf-40cd-8dcd-3b630bdc1bbd1033.mspx

AD adapter password change registry

The AD adapter maintains a registry of all password changes that it has initiated from the Identity Manager server. This registry is checked by the reverse password synch module before the reverse password synch module processes a changed password in order to stop the mechanism from looping.

The HKLM\SOFTWARE\Access360\ADAgent\Specific\PasswordChanges registry key value holds the table of password changes initiated by the adapter. This contains a user ID and hashed copy of the password.

You should not edit the registry key value, but you can check it to help you with problem determination.

Mapping AD Base Points to services

The reverse password synch module needs to know to which service these accounts are tied in Identity Manager, so it knows which password policy to apply and how to find the person who owns the accounts. The reverse password synch module can monitor multiple AD Base Points and map them to different Identity Manager Service definitions. However, the Base Point <-> Service Target DN definitions in the reverse password synch configuration must match the definitions in the AD adapter.

You can see details about setting the correct Service DN in the Tivoli Support Technote “Passwd Sync Agent - formulating targetDN for the service name” at:

http://www.ibm.com/support/docview.wss?uid=swg21161718

Also, see the *IBM Tivoli Identity Manager: Password Synchronization for Active Directory Plug-in Installation and Configuration Guide*, SC23-5268-00, for examples of the Base Point and Service Target DN definition.

Security and SSL

There is a discussion of SSL and how it relates to the reverse password synch module in the *IBM Tivoli Identity Manager: Password Synchronization for Active Directory Plug-in Installation and Configuration Guide*, SC23-5268-00. The information in Chapter 3, “SSL Configuration” relates more to the DAML adapters/agents than the reverse password synch

module. So, we are adding a short discussion below to focus on the reverse password synchronization.

The reverse password synch module connects to the Identity Manager server through HTTPS (for example, https://server:9443/passwordsynch/synch). It acts as an SSL client, just as any Web browser that connects to a Web server over HTTPS. The Web server acts as the SSL server in the interaction. When the reverse password synch module connects to the Web server HTTPS port, the Web server returns a certificate. With a Web browser, if the certificate is not signed by a known signing authority or certificate authority (CA), the Web server prompts the user to verify the certificate signer. The reverse password synch module does not have a user to verify the certificate, so it must have the signing authority certificate defined to it.

Example 1 is a pwdsynch.log, which shows the module trying to access the signing authority cert.

Example 1 pwdsynch.log of the module trying to access the signing authority cert

```
Tue Jan 09 21:50:28 00000334 Initializing SSL - version: OpenSSL 0.9.7d 17 Mar
2004
Tue Jan 09 21:50:28 00000334 Number of SSL locks to be allocated: 34
Tue Jan 09 21:50:28 00000334 Registering thread identifier function...
Tue Jan 09 21:50:28 00000334 Registering thread lock/unlock function...
Tue Jan 09 21:50:28 00000334 Creating new client side SSL context...
Tue Jan 09 21:50:28 00000334 Loading CA cert list
'C:\Tivoli\PasswordSynch\data\DamlCACerts.pem'
Tue Jan 09 21:50:28 00000334 Unable to load CA certificate
'C:\Tivoli\PasswordSynch\data\DamlCACerts.pem'
```

In this case, the reverse password synch module looks for a signing authority cert in c:\Tivoli\PasswordSynch\data\DamlCACerts.pem. This is the hardcoded file that the reverse password synch module uses; you cannot change this file.

You use the CertTool utility to define signing authority CA certs to the reverse password synch modules. The following sections in Chapter 3 of the *IBM Tivoli Identity Manager: Password Synchronization for Active Directory Plug-in Installation and Configuration Guide*, SC23-5268-00, are relevant for this:

- Installing a CA Certificate (page 18) to install a .pem file that contains the signing authority CA file for the certs being issued by the HTTP or HTTPS server.
- Viewing CA Certificates (page 19) to see which signing authority CA certificates are defined to the reverse password synch module
- Deleting a CA certificate (page 19) to remove a signing authority CA certificate from the reverse password synch module

So to load a CA, you run CertTool and install the file. Example 2 shows you how to load a CA.

Example 2 Running CertTool to install a file to load a CA

```
C:\Tivoli\PasswordSynch\bin> certtool –ag PwdSync
  Main menu - Configuring agent: PwdSync
  ------------------------------
  A. Generate private key and certificate request
  B. Install certificate from file
  C. Install certificate and key from PKCS12 file
  D. View current installed certificate
  E. List CA certificates
```

```
  F. Install a CA certificate
  G. Delete a CA certificate
  H. List registered certificates
  I. Register certificate
  J. Unregister a certificate
  K. Export certificate and key to PKCS12 file
  X. Quit
 Choice: F
 Enter name of certificate file: z:\ctemp\CA.pem
Subject: /C=US/O=IBM
Install this CA (Y/N)? y
```

This updates (or creates if it does not exist) the DamlCACerts.pem (in c:\Tivoli\PasswordSynch\data).

Upon restarting the server, you should see a success message in the log that is similar to Example 3.

Example 3 Success message in log

```
Tue Jan 09 22:16:49 0000033c Initializing SSL - version: OpenSSL 0.9.7d 17 Mar
2004
Tue Jan 09 22:16:49 0000033c Number of SSL locks to be allocated: 34
Tue Jan 09 22:16:49 0000033c Registering thread identifier function...
Tue Jan 09 22:16:49 0000033c Registering thread lock/unlock function...
Tue Jan 09 22:16:49 0000033c Creating new client side SSL context...
Tue Jan 09 22:16:49 0000033c Loading CA cert list
'C:\Tivoli\PasswordSynch\data\DamlCACerts.pem'
Tue Jan 09 22:16:49 0000033c Loaded CA Certificate: /C=US/O=IBM
```

The only time that you need to load a normal certificate (not a signing certificate) into the reverse password synch module is when the HTTP server is configured to require client side certificates. This is the exception rather than the rule. In this case, you need to load the cert into the reverse password synch module using CertTool (this time using option I. Register certificate) and ensure that the HTTP server is configured to recognize the cert.

Maintenance and logging

This section looks at the maintenance and logging aspects of the Windows reverse password synch module.

Maintenance

There is very little to be concerned about regarding maintaining the module. There is only one executable and two utilities. After you install the module, you can easily update the module.

If logging is enabled, you need to monitor the logfile size, and because it runs on Windows, you are unlikely to fill up a disk.

Tuning of the module is limited. The only tuning setting is the maximum parallel requests setting (registry: MaxParallelRequests, pfconfig: Maximum No. of Password Change Requests Allowed). This is the number of threads that the module uses.

If the Identity Manager Server SSL certs are set to expire, you might need to maintain the CA certs that are used by the reverse password synch module.

Logging

The reverse password synch module produces a single logfile, PwdSync.log, found in the <*installdir*>\log folder (such as c:\Tivoli\PasswordSynch\log).

Figure 4 shows an example of the log.

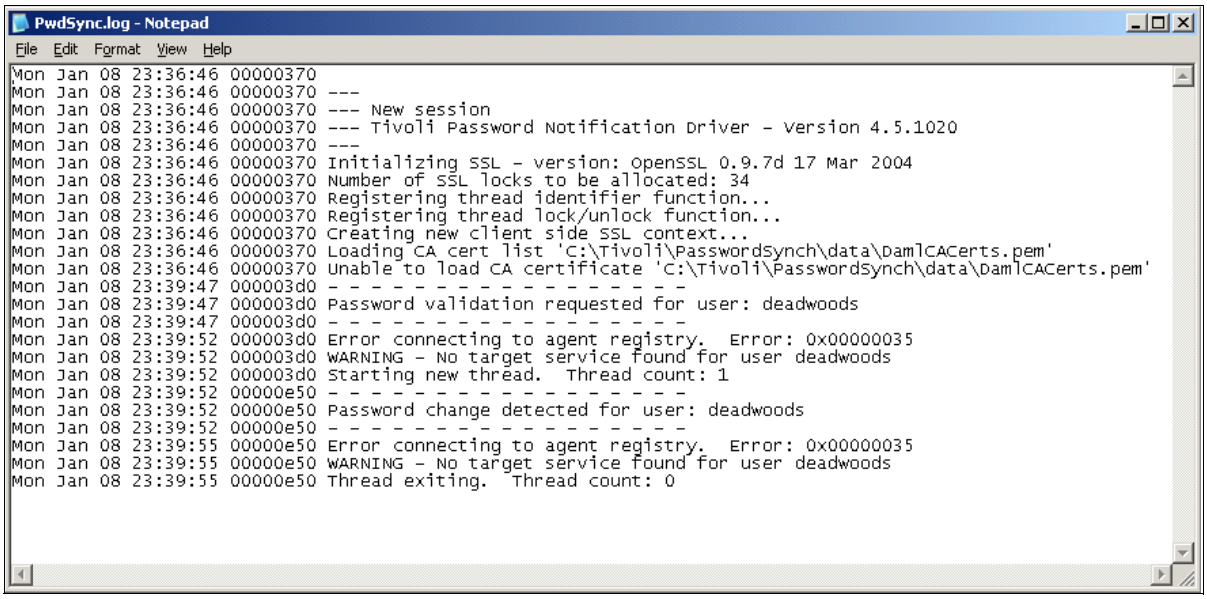

Figure 4 PwdSync.log file produced by the reverse password synch module

The PwdSync.log file contains information about the module (such as version number and startup messages) and entries for each password change operation.

This file is extremely useful when you diagnose problems with the module. You need to also look at both:

- The Identity Manager AD adapter log (C:\Tivoli\Agents\ADAgent\log\WinADAgent.log)
- The Identity Manager server log:
  - **itim.log** for Identity Manager V4.5 (under the WebSphere Application Server directories)
  - **msg.log** for Identity Manager Express V4.6 and Identity Manager V4.6 (now found in the tivoli\common\CTGIM\logs directory)

All three logs cover the complete reverse password synchronization cycle. A problem related to changing passwords might be in the reverse password synch module, the Identity Manager server, or the AD adapter. If you checking all three logs, you can identify where the problem exists.

Common problems

This section lists some of the common problems that you might encounter with the Windows reverse password synch modules.

Incorrect host name and port definitions

There are not many configuration settings for the reverse password synch module. The Identity Manager Web server host name and HTTPS port are defined so that the reverse password synch module can contact Identity Manager for synchronizing passwords and checking policy. If these are incorrectly defined, you will see errors in the reverse password synch logs.

You can check the reverse password synch configuration by performing a basic ping test. Using a Web browser, point to:

`https://<server>:<https_port>/passwordsynch/synch`

In this Web address, <*server*> and <*https_port*> are as you have defined them in pfconfig. If the server and https_port are correct, you see an error message indicating a malformed XML and a string similar to Example 4.

Example 4 Error message showing malformed XML

```
<SYNCH_PSWDS_RESP code="failure" desc="The root element is required in a
well-formed document." />
or
<SYNCH_PSWDS_RESP code="failure" desc="Premature end of file." />
```

This indicates that the servlet is found, and the server and the HTTP port are correct.

If you get a "`page not found message`", there might be a problem with the servlet. If you can log in to Identity Manager using the same Web address, but you can get to the normal Identity Manager login page using:

`http://<server>:<http_port>/enrole`

It is likely that there is a problem with the servlet. If you cannot get to the Identity Manager login page, there is likely a problem with the Identity Manager server or application.

If the HTTP connection works, but an HTTPS connection fails to the Identity Manager login page at:

`https://<server>:<https_port>/enrole`

The HTTP server might not be correctly configured for HTTPS.

Incorrect SSL certs

In "Security and SSL" on page 9, we described how SSL works with the reverse password synch module and listed one of the error messages that might appear in the reverse password synch log. If you encounter SSL cert errors, you can use the CertTool to check what CA certs (if any) are loaded into the reverse password synch module.

You can also use the HTTPS Web address to check if SSL is configured for the server and if the cert it presents to the browser matches the cert defined to the reverse password synch module:

`https://<server>:<https_port>/passwordsynch/synch`

You might need to extract the CA cert from the HTTPS cert presented to the browser (different browsers have different approaches to this) and import that into the reverse password synch module using CertTool.

Incorrect service definition

If the reverse password synch module has an incorrect service definition defined, you see a message in the log similar to Example 5 on page 14.

Example 5 Message in the log regarding an incorrect service definition

```
Tue Jan 09 22:35:20 00000390 - - - - - - - - - - - - - - - - - -
Tue Jan 09 22:35:20 00000390 Password validation requested for user: deadwoods
Tue Jan 09 22:35:20 00000390 - - - - - - - - - - - - - - - - - -
Tue Jan 09 22:35:25 00000390 Error connecting to agent registry.  Error:
0x00000035
Tue Jan 09 22:35:25 00000390 WARNING - No target service found for user deadwoods
```

This indicates a problem with the services defined for the module. The AD reverse password synch module might have multiple services defined (each mapped to a different AD base point).

Details of how to set the correct service DN can be found in the Tivoli Support Technote “Passwd Sync Agent - formulating targetDN for the service name” at:

http://www-1.ibm.com/support/docview.wss?uid=swg21161718

Also, see the *IBM Tivoli Identity Manager: Password Synchronization for Active Directory Plug-in Installation and Configuration Guide*, SC23-5268-00, for examples of the Base Point and Service Target DN definition.

Incorrect principal user ID definition

The reverse password synch module (all of them, not just the Windows one) uses an Identity Manager account to log in to Identity Manager (called the Identity Manager principal on the configuration GUI).

You might get problems, such as:

- If the principal account is locked out in Identity Manager, the pwdsync.log displays a message similar to “`invalid account`.”
- If the access control information (ACI) is not set up correctly, the password is not synchronized.

At a minimum, the sync user (principal) needs to be granted permission for password synchronization:

- Search for the account that triggered the password synchronization.
- Search for that account’s owner.
- Search for any accounts that should have their passwords synchronized.
- Modify those same accounts, with write access to their password attributes.

If you want to use password policy verification, make sure that the principal user ID is an Identity Manager administrator (a member of the sys admin group). This is not documented anywhere.

Note that this information applies to all reverse password synch modules, not just the AD module.

Remote registry access

If the reverse password synch module is deployed to a different server than the provisioning adapter, such as the AD adapter, the account running the reverse password synch module needs to have the appropriate access rights in order to access the registry on the provisioning adapter machine.

There are different settings depending on whether the OS is Windows NT®, Windows 2000 Server, or Windows Server 2003. For the Windows Server 2003 settings, see the Technote “ITIM Active Directory® Password Sync - Error opening registry key. Error: 0x00000005” at:

http://www-1.ibm.com/support/docview.wss?uid=swg21226812

This concludes the section on the Windows AD Reverse Password Synch module.

Other Identity Manager reverse password synch modules

In addition to the Windows Reverse Password Synch module, there are a number of other reverse password synch modules shipped with Identity Manager adapters. At the time of writing this Redpaper (May 2007), the adapters listed in shipped with reverse password synch modules.

Table 1 Adapters that ship with reverse password synch modules

Adapter	Version	Pwdsync	Version
MS Windows AD	4.6.13	Windows	4.6.6 (June 2005)
IBM AIX®	4.6.5	AIX	4.6.0 (June 2005)
IBM i5/OS®	4.6.3	System i™	4.6.0 (June 2005)
IBM RACF®	4.6.2	RACF	1.0.0 (December 2003)
IBM Tivoli Access Manager for e-business	4.6.*n* [1]	Access Manager for e-business 4.1 [2]	4.6.0 (March 2006)
		Access Manager for e-business 5.1/6.0 [2]	4.6.2 (February 2006)
		Access Manager for e-business 5.1 for Identity Manager Express [3]	4.6.3 (March 2006)
		Access Manager for e-business 6.0 for Identity Manager Express [3]	4.6.3 (March 2006)
IBM i5/OS	4.6.0	System i	4.6.1 (May 2006)
UNIX/Linux® Remote	4.6.2	AIX (only) [4]	4.6.1 (February 2006)

1. There are different adapters for Access Manager for e-business, several at 4.6.4 and several at 4.6.5.
2. There are different password synch modules that ship with the Access Manager for e-business adapters for different versions of Access Manager for e-business.
3. There are separate reverse password synch modules to use the Access Manager for e-business adapters with Identity Manager Express.
4. The UNIX/Linux RMI (remote) adapter only supports reverse password synch on AIX.

After the Windows module, the Access Manager for e-business module is the most widely deployed. The next sections summarize these modules. The focus is on the Access Manager for e-business module, because it is the most widely deployed module.

Access Manager for e-business Reverse Password Synch module

The Access Manager for e-business Reverse Password Synch module performs the same functions as the Windows module, but it is implemented differently. The password synch

module is hooked into WebSEAL or the Web Plug-ins; the Access Manager adapter uses the Access Manager Admin APIs to apply changes to the Access Manager user repository. The module does not have the same issues with looping that the AD adapter has, which makes deployment much easier.

Note this section discusses Access Manager for e-business WebSEAL, but the implementation applies equally to the Access Manager for e-business Web Plug-ins.

Figure 0-5, which is in the *Tivoli Access Manager 5.1 Password Synchronization Adapter Installation and Configuration Guide,* shows the major components in the deployment and how they interact.

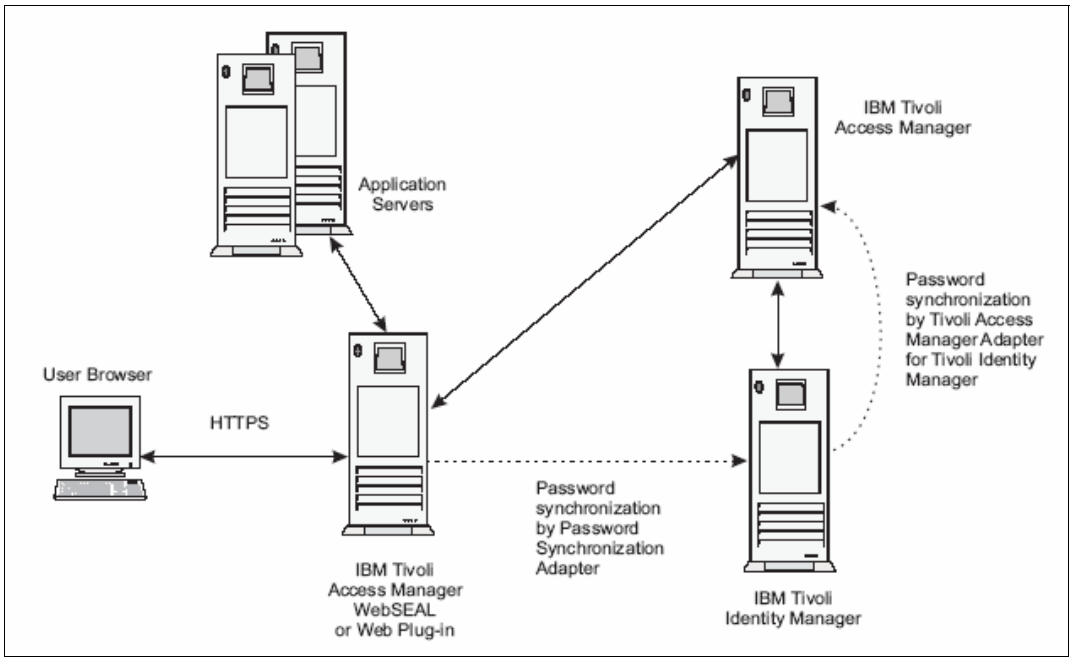

Figure 0-5 Password synchronization deployment components

Chapter 1, “Overview”, of the *Tivoli Access Manager 5.1 Password Synchronization Adapter Installation and Configuration Guide* contains a great overview of the product, including the code that is deployed and how the code is implemented. The server code is the same as the code that is used by all other reverse password synch modules. The client code, the components that are installed on the WebSEAL machines, is specific to the module. There are different versions of the module for different versions of Access Manager for e-business and whether you use Identity Manager or Identity Manager Express.

The module hooks into WebSEAL using the webseald.conf file. There are password strength and password processing settings under the [authentication-mechanisms] stanza in the file (the configuration is described in the *Installation and Configuration guide*).

It is important to check the passwd-strength and post-pwdchg-process settings:

- Do they use the correct libraries (one library is for checking and the other library is for synchronization)?
- Do they use the correct last argument (“check” or “synch”)?

Also, the service DN must be correctly specified (see “Incorrect service definition” on page 13).

You must configure the adapter to talk to the Identity Manager server using HTTPS (see “Security and SSL” on page 9). The adapter is configured differently than the AD module, and the steps are described in detail in the *Installation and Configuration Guide*. With the Access Manager reverse password synch module, you use a keytab file to contain certificates.

The configuration settings, such as the Identity Manager server host and IP address, are held in a configuration file (passwdsync.conf) rather than in the registry (as in the AD module).

Logging is defined by settings in the passwdsync.conf file: logfile and log level. Log level can be “verbose” or “debug” (or omitted). If nothing is specified for either setting, the WebSEAL logfile is used. There are troubleshooting tips and common problems listed in the *Installation and Configuration Guide*.

AIX Reverse Password Synch module

The AIX Reverse Password Synch module performs the same functions as the other reverse password synch modules but is implemented differently. The password synch module is hooked into the AIX login modules. It is deployed to the same servers as the AIX (Provisioning) adapters.

Configuration information for the AIX module is held in a file, itim_aix_passwd_sync.conf (found in the /etc directory). The settings are maintained through the psConfig utility (normally in usr/tivoli/PwdSync/bin). The config settings are similar to the other reverse password synch modules, such as Identity Manager server host and port, service DN, Identity Manager principal and password, and log settings.

The psConfig utility manages the SSL certificates by calling a version of the CertTool utility (see “Security and SSL” on page 9). As with the other reverse password synch modules, the AIX module must have the signing authority (CA) cert defined to it. You only need to create a certificate for the module (options A-C in Managing Certificates) if the HTTP server is defined to require client side certificates.

The key difference between V4.6.1 (supplied with the UNIX/Linux RMI adapter) and V4.6.0 (supplied with the AIX DAML adapter) is support for Identity Manager Express. The Installation and Configuration Guide states the same information.

System i (i5/OS) Reverse Password Synch module

You must install the i5/OS Reverse Password Synch Plug-in on the System i server before the Identity Manager will accept password changes from the System i Password Change user interface.

You must also install the System i FTP Agent (provisioning adapter) on the same server as the i5/OS Reverse Password Synch Plug-in.

See the *Tivoli Access Manager Password Synchronization Adapter Installation and Configuration Guide*, SC32-1756-02 for installation prerequisites and steps. It contains the relevant i5/OS commands to configure the module to intercept i5/OS password changes.

As mentioned before with the AD Reverse Password Synch module, if you need additional information about certificates and SSL configuration in relation to reverse password synchronization see “Security and SSL” on page 9 (in addition to the *Tivoli Access Manager Password Synchronization Adapter Installation and Configuration Guide*, SC32-1756-02, Chapter 3, “Configuring SSL Authentication for the Adapter”).

The relevant section of the *Tivoli Access Manager Password Synchronization Adapter Installation and Configuration Guide*, SC32-1756-02 is “Installing CA certificates” on page 10.

This section contains the steps to copy (ftp) the Identity Manager server cert to the i5/OS machine and then use i5/OS utilities to load it into the system.

Note: The *Tivoli Access Manager Password Synchronization Adapter Installation and Configuration Guide*, SC32-1756-02 lists a 360demo.cer, which is a sample certificate. Do not use this sample cert for your production environment. Use 360demo.cer only for demonstration systems.

There is also a separate document shipped with the adapter, *as400cert.doc*, which details the steps. Unfortunately, the document does not seem to be complete.

The module uses i5/OS utilities to manage the CA certs; you do not need to create keystores or use the CertTool as you do with other reverse password synch modules.

RACF Reverse Password Synch module

The RACF adapter ships with an Tivoli Directory Integrator-based reverse password synch module. Unlike the other modules, this module requires significant configuration, which can involve modifying the Tivoli Directory Integrator AssemblyLines.

The sample Tivoli Directory Integrator configuration file supplied for this module contains a z/OS® Changelog Event Handler and custom AssemblyLine. The AssemblyLine gets the new password from RACF (using RACF calls in the RACF connector), captures the changed password (and user ID), and sends both the new and changed passwords to the Identity Manager server (using the Identity Manager Password Synch Connector). The AssemblyLine is configured to read the RACF entry that changed by using the RACF LDAP interface, decode the password, and forward the user name and password to Identity Manager. The password retrieved from RACF is encrypted using a key that must be made available to Tivoli Directory Integrator.

You can use this sample configuration for your own RACF Reverse Password Synch module implementation. We are not aware of any way to capture a changed RACF password other than through the LDAP changelog when RACF is configured to use LDAP.

See the readme.txt document that ships with the module for more details, including the prerequisites, installation description, and configuration instructions.

Also, see the Tivoli Directory Integrator documentation describing the various connectors and the other Tivoli Directory Integrator components that are used. The *IBM Tivoli Directory Integrator 6.1.1: Reference Guide,* SC32-2566-01, lists all of the components and their use, such as the z/OS Changelog Connector.

Reverse password synch with Tivoli Directory Integrator

Tivoli Directory Integrator provides a number of plug-ins to capture passwords from different sources. You can use these plug-ins in Tivoli Directory Integrator AssemblyLines to synchronize passwords with other repositories, which includes the Identity Manager Server.

The Tivoli Directory Integrator Password Synch plug-ins available with Tivoli Directory Integrator V6.1 are:

- Password Synchronizer for Windows NT, Windows 2000 Server, Windows XP intercepts the Windows login password change.

- Password Synchronizer for IBM Tivoli Directory Server intercepts IBM Tivoli Directory Server password changes.
- Password Synchronizer for Sun ONE Directory Server intercepts Sun ONE Directory Server password changes.
- Password Synchronizer for Domino® intercepts changes of the HTTP password for Lotus® Notes® users.
- Password Synchronizer for UNIX® and Linux intercepts changes of UNIX and Linux user passwords (Pluggable Authentication Module).

Some of these plug-ins duplicate the functionality of existing Identity Manager reverse password synch modules, such as Windows. Other plug-ins provide the ability to create custom reverse password synch modules, such as the plug-in for Domino.

You can obtain a sample reverse password synch module using Tivoli Directory Integrator components with the RACF adapter (see “RACF Reverse Password Synch module” on page 18). You can use this sample reverse password synch module to build other modules.

For more information, see the *IBM Tivoli Directory Integrator: Password Synchronization Plug-in Guide*. It includes a good chapter (Chapter 10) about Identity Manager Integration.

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.

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.

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.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document REDP-4299-00 was created or updated on May 14, 2007.

Send us your comments in one of the following ways:
- Use the online **Contact us** review Redbooks form found at:
  ibm.com/redbooks
- Send your comments in an e-mail to:
  redbooks@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Redbooks (logo) ®	Domino®	RACF®
i5/OS®	IBM®	System i™
z/OS®	Lotus Notes®	Tivoli®
Access360®	Lotus®	WebSphere®
AIX®	Notes®	

The following terms are trademarks of other companies:

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

Active Directory, Windows NT, Windows Server, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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