ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

Managing Security using Password Synchronization

Himanshu Taneja
himanshu.taneja24@gmail.com

Abstract -What if you need to memorize n number of passwords for getting access to n number of resources across an organization? Users may face many problems in remembering their passwords which will result into raising number of service desk calls for password-resetting which in turn results into wastage of precious-time and hence money of an organization. This paper deals with Password Synchronization issue and provides a solution to this problem using IBM Tivoli Identity Manager. The users need not to remember number of passwords for the different accounts on different resources, so the cost as well as the security problem will be reduced.

***Index Terms*— Identity, Identity Management, Password Security, Password Synchronization.**

I. INTRODUCTION

These days an Enterprise require a solution that provides centralized user management, from on-board till exit. With the increase in number of applications, users are forced to remember multiple IDs and passwords. To create an improved user experience and simplify administration, enterprises require a centralized mechanism to manage the authentication of users. Same password is assigned to the user for using different resources or different services. The users need not to remember number of passwords for the different accounts on different resources, so the cost as well as the security problem will be reduced.

It involves implementing password synchronization through reverse password synchronization module, as the native password changes that already taken place on a common system (Microsoft Active Directory) are reflected through the password management system to other systems and applications. It also involves resetting the password by the users by their own. It will allow users who have forgotten there password to repair their problem, without calling the helpdesk. This can be done by establishing the user's identity, without using their forgotten password, by answering a series of challenge-response questions. Also a common password policy will be defined and will be followed by all the resources to generate the passwords.

II. ARCHITECTURE

The user desktops are Windows based. All users log in to Microsoft Active Directory in order to start a session and access corporate applications. Since password reset has become a problem because of the amount of users who forget their passwords, and with the implementation of the new security policy for passwords, reset password is becoming a very hard task. Now that we need to implement password synchronization between corporate applications, users just have to remember one password. In case a user needs to change a password, we want the user to change the password on her own, using the Microsoft Windows user interface, because the user already knows how to do it.

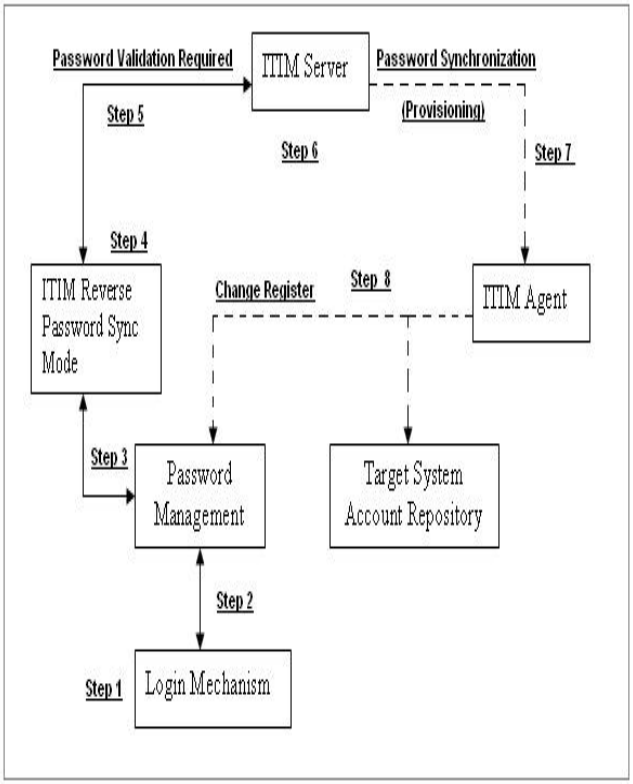

Fig. 1. Architecture of Password Synchronization

➢ **Following steps describe the flow when Windows prompts to Change the password (In an AD Domain):**

➢ **Step 1:** Enter new password into the normal Windows Change Password dialog and press OK.

➢ **Step 2:** The workstation contacts a domain controller and passes the user credentials (User ID and Password).

➢ **Step 3:** The domain controller performs its password checks and passes control to the Identity Manager Active Directory (AD) reverse password Synchronization module.

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

➢ **Step 4:** The AD reverse password synchronization module determines the base point in AD and uses this to determine the related Identity Manager Service Domain Name (DN) (from password sync configuration).

➢ **Step 5:** The password change request is sent from the reverse password synch module to the Tivoli Identity Manager (ITIM) Password synch/synch servlet.

➢ **Step 6:** 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 password synchronization is enabled, it lists the accounts that are owned, determines the combined password rules for all the accounts, and checks against those rules.

➢ **Step 7:** If the password change was successful, continue into Windows; otherwise, get prompted for another new password.

➢ **Step 8:** If the password synch is enabled, it also sets the password on all the other accounts associated with. This generates provisioning requests down to the systems holding these accounts using the normal Identity Manager provisioning mechanism.

Overview of AD Adapter: The Windows Active Directory (WinAD) Adapter is designed to create and manage Active Directory accounts within a Windows 2000 or Windows2003 domain. This Adapter does not create or manage local system accounts. IBM recommends the installation of this Adapter on a Windows 2000, Windows 2003 or XP workstation within the domain being managed. Typically, one adapter is installed per domain, but the WinAD Adapter may be configured to support both sub-domains and multiple domains through the Base Point Feature on the WinAD Service Form. The optimum deployment configuration is based, in part, on the topology of your windows domain, but the primary factor is the planned structure of our Identity Manager Provisioning Policies and Approval Workflow process. The WinAD Adapter is a powerful tool that requires Administrator Level authority. The Adapter operates much like a human system administrator, creating Active Directory accounts, Exchange mailboxes, and Home Directories. Operations requested from the Identity Manager server will fail if the Adapter is not given sufficient authority to perform the requested task. IBM recommends that this Adapter run with local or domain level administrative permissions.

III. REVERSE PASSWORD SYNCHRONIZATION

Reverse password synchronization is where a password change on one of the target systems, such as in a Windows Domain Controller, 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 we have deployed a single-sign on (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). We can enable both of these functions, one only, or none of them.

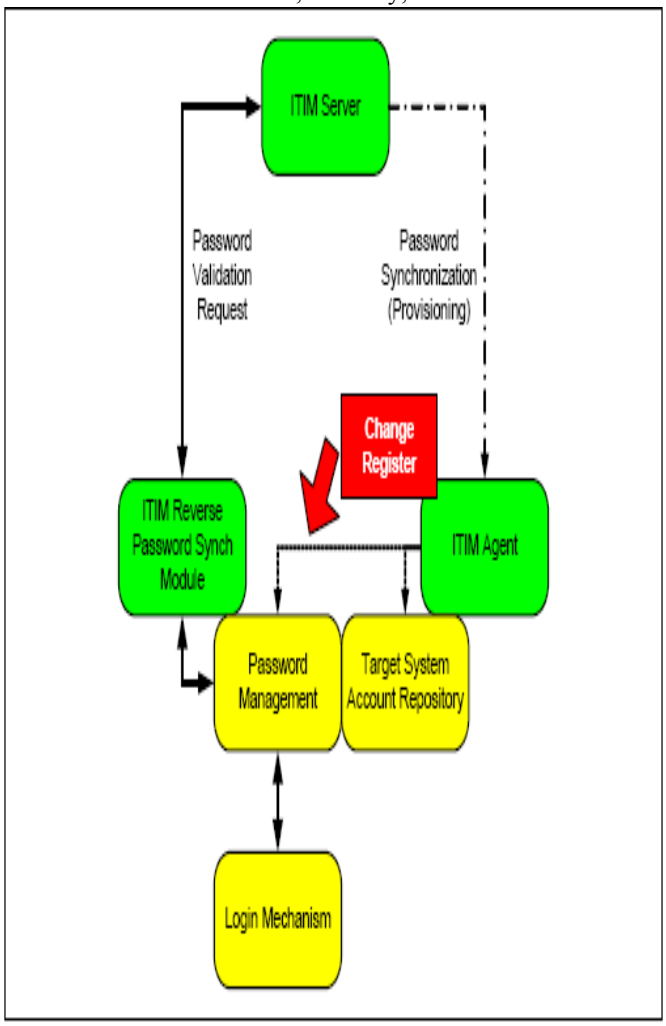

Fig. 2. Reverse Password synch mechanism

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 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

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 2, February 2012

through their provisioning adapter (that is, the Identity Manager adapter).

IV. CONCLUSION

In this paper, we present the design and implementation of Password Synchronization across any organization using IBM Tivoli Identity Manager. It assigns a common password to a user for accessing different resources allocated to the user in an organization. It reduces number of helpdesk calls which results into less user frustration and hence more user satisfaction which is the primary goal of any organization to provide the better working environment for the employees that further helps in achieving a Win-Win strategy for all.

REFERENCES

[1] Axel Buecker, David Edwards," Tivoli Identity Manager and Reverse Password Synch Modules", © Copyright IBM Corp. 2007. All rights reserved.

[2] Chen Zhao, Yang Chen, Dawei Xu, Nuer Maimaiti Heilili, and Zuoquan Lin, "Integrative Security Management for Web-Based Enterprise Applications" WAIM 2005, LNCS 3739, pp. 618 – 625, 2005. © Springer-Verlag Berlin Heidelberg 2005.

[3] Fig. 2. Reverse Password synch mechanism, Axel Buecker, David Edwards, "Tivoli Identity Manager and Reverse Password Synch Modules", pp. 3.© Copyright IBM Corp. 2007.

[4] http://en.wikipedia.org/wiki/Password_synchronization.

[5] http://download.oracle.com/docs/cd/E19225-01/821-0094/821-0094.pdf, Chapter-11.

AUTHOR BIOGRAPHY

Himanshu Taneja received Master degree in Computer Applications, with honors from Punjab University, Chandigarh, India in 2008. Her research interests include security and privacy of Users across the organization. She currently works in the National Institute of Technology, Kurukshetra, and Haryana, India. Her previous work is associated with Wipro Technologies, Gurgaon, Haryana, India as a Software engineer in Enterprise Security and Services domain.