International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015
ISSN 2091-2730

Mac OS X and Directory Services Integration

Neha Setia[1] and Tarun Dalal[2]

[1]M.Tech Scholor, CBS Group of Institutions, CSE Department, MDU Rohtak, India
setia_neha@yahoo.co.in

[2]Assistant Professor, CBS Group of Institutions, CSE Department, MDU Rohtak, India

Tarundalal88@gmail.com

Abstract— Market share in the enterprise is largely dominated by Microsoft -- specifically, the reliance on the Windows Server family line to manage network resources, align desktops with corporate security policies, and maintain the flow of production amongst all the employees at a given organization. The process of administering all these systems -- desktops and servers alike -- are relatively straight-forward in a homogeneous environment, but what happens when OS X is introduced to the enterprise in the form of a sleek, shiny new MacBook Air or iMac? The objective of this paper is to provide the solution of this question. Supporting Mac users can be a challenge to systems administrators in a Windows Active Directory environment. Although Apple has used Samba to make it easy for Macs to browse and access shares and printers hosted by Windows servers using Microsoft's server message block (SMB) protocol, true Active Directory integration requires more than just access to resources. The objective of this project is to provide a way to integrate Mac devices with Windows Server Active Directory. Although Apple has provided way to bind Mac with AD but this project would also take this integration to next level by considering other options available to integrate Mac with directory services.

Keywords— Mac OS X, ADDS, Network Domain, Kerberos, Domain Server, Active Directory, Open Directory.

1. INTRODUCTION

Mac OS X is a powerful Apple desktop and portable computers operating system. Since it's introduction in 2001, OS X has become an increasingly attractive alternative to other operating systems because of its combination of innovative technologies. Apple, third-party developers, and security experts build OS X on a foundation of open source components that have been through decades of intense scrutiny. Apple support for directory services enable Mac clients and servers to integrate smoothly into existing Active Directory environment and provides the option of deploying a single, directory services infrastructure that can support both Macs and Windows clients.

Apple's implementation of a centralized directory service is called Open Directory. Integrated into the foundation of OS X, Open Directory is responsible for providing directory and network authentication services for both OS X clients and OS X Server. Open Directory uses open-standard protocols such as LDAP, Kerberos, and SASL. Although Apple provides its own native, directory services platform through Open Directory, OS X supports access to a variety of other

platforms, including Active Directory. While every Active Directory installation is different, OS X integrates well with the vast majority of platforms with minimal effort.

OS X offers Active Directory integration through a directory service. With this support, the user doesn't need to maintain a separate directory or separate user records to support OS X systems. Users can move between different computers, while still adhering to enterprise policies for strong authentication and password-protected access to network resources.

2. ACTIVE DIRECTORY

Active Directory is Microsoft's trademarked directory service, an integral part of the Windows 2000 architecture. Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories. Active Directory is designed especially for distributed networking environments.

Active Directory features include:

- The capability for secure extension of network operations to the Web
- A hierarchical organization that provides a single point of access for system administration (management of user accounts, clients, servers, and applications, for example) to reduce redundancy and errors
- An object-oriented storage organization, which allows easier access to information
- Support for the Lightweight Directory Access Protocol (LDAP) to enable inter-directory operability
- Designed to be both forward compatible and backward compatible.

Active Directory is applicable where Network administrators write scripts and applications that access Active Directory Domain Services to automate common administrative tasks, such as adding users and groups, managing printers, and setting permissions for network resources.

Independent software vendors and end-user developers can use Active Directory Domain Services programming to directory-enable their products and applications. Services can publish themselves in Active Directory Domain Services; clients can use Active Directory Domain Services to find services, and both can use Active Directory Domain Services to locate and work with other objects on a network.

3. OPEN DIRECTORY

Server App offers an LDAP directory service implementation from Apple Inc. Open Directory comes as service with server app which can be configured for the purpose of centralized management of global Macs. It Provide a centralized location to store information about users, groups, and other resources, and integrate with existing directory services. Mac OS X Server's Open Directory provides directory and authentication services for mixed networks of Mac OS X, Windows, and UNIX computers.

Open Directory uses OpenLDAP, the open source implementation of Lightweight Directory Access Protocol (LDAP), to provide directory services. It's compatible with other standards-based LDAP servers, and can be integrated with proprietary services such as Microsoft's Active Directory and Novell's eDirectory. For the LDAP database back end, Open Directory uses the open source Berkeley Database. It's a highly scalable database for high-performance indexing of hundreds of thousands of user accounts and other records.

Open Directory plug-ins enable a Mac OS X client or Mac OS X Server computer to read and write authoritative information about users and network resources from any LDAP server—even Microsoft's proprietary Active Directory. The server can also access records in legacy directories such as NIS and local BSD configuration files (/etc). Open Directory also provides authentication service. It can securely store and validate the passwords of users who want to log in to client computers on your network or to use other network resources that require authentication.

4. WHY MAC OS X AND DIRECTORY SERVICE INTEGRATION IS REQUIRED

Below points can describe the purpose of integrating Macs with Directory Services:

- Handling of thousands of Mac in Enterprise Environment.
- To have Single Sign On support.
- To enable network users to login to any Mac on the network.
- Manage all administrative work on all Macs.
- It is important to handle the Macs via Active Directory to manage them centrally.
- Using Apple solutions to bind Macs with Windows Server Active Directory.
- Identifying third party solutions to bind Macs with Windows Server Active Directory.
- Implementing Group Policies on all Macs using Active Directory.
- Using Group Policies on Mac, you can control thousands of actions on thousands of Mac remotely.

- The objective of work is implement Mac and Active Directory integration for high end control over the remote Macs of an enterprise.

When fully integrated with Active Directory or Open Directory, OS X offers a complete managed environment where users can:

- Access any Mac in the integrated environment using the same credentials they would use to access Windows PCs.
- Require adherence to the Active Directory password policies.
- Benefit from single sign-on access to Active Directory resources through Kerberos.
- Users can have local home directories while maintaining access to the
- Network-based home folder specified in their Active Directory record.

5. MAC OS X AND ACTIVE DIRECTORY BINDING

The lowest-cost solution is to use Apple's built-in Active Directory support. Beginning in Mac OS X Panther (10.3), Apple introduced a plug-in to its Directory Access utility that allows you to configure authentication against Active Directory. Apple's Active Directory plug-in uses LDAP to query Active Directory. The Active Directory plug-in works fairly well. It supports forests with multiple domains, domain controller fail-over and can auto mount a user's home directory. It can also grant users administrator access to a Mac workstation based on their Active Directory group membership.

Below steps need to be followed to bind a Mac OS X with existing active directory domain services.

1. On the Mac, go to System Preferences, and click on the padlock to authenticate as an Administrator.
2. Enter your admin-level credentials to authenticate when prompted.
3. Select Login Options and then click the 'Join' button next to network account server.
4. In the server drop down menu, enter the fully qualified domain name of the windows domain you want to bind to the Mac and click Ok.
5. Next, you need to enter your domain level credentials in order to proceed with the binding process. Make sure that computer name is unique and formatted properly because this will be the name that will be created for computer object in ADDS. Then click OK to proceed for enrollment.
6. Upon successful binding, the window will close and the Users and Group preferences will remain open, but a small green dot will appear next to network account server to indicate connectivity to the domain.

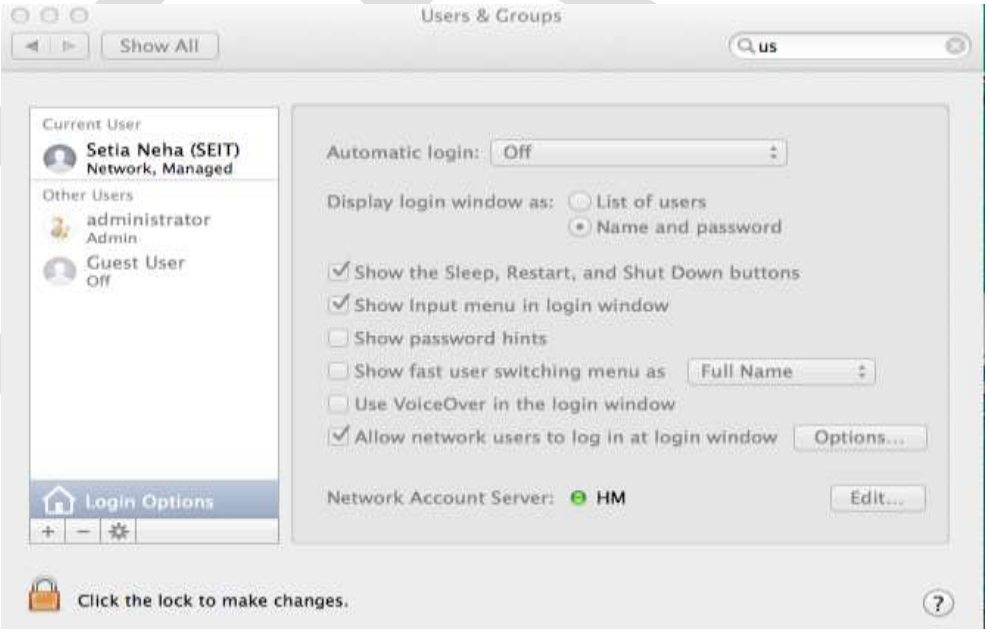

Figure 1: Mac joined to HM domain

Note*: By default, Windows will automatically create the computer object account in ADDS if one does not already exist. However, domain or enterprise admins may (and often do) restrict this as a security feature to curb random nodes from being joined to the domain. Additionally, Organizational Units (OU) may be created as a form to compartmentalize ADDS objects by one or more classifications or departments. Many enterprises will utilize OUs as a means to organize

objects and accounts separately from the items created by default when a domain controller is promoted and ADDS is created.

6. MAC OS X AND OPEN DIRECTORY BINDING

Open Directory comes as service with Apple Server application which is able to use DNS service records and site information stored within Active Directory to find and communicate with the most appropriate domain controllers (typically ones in close proximity in multisite networks). By querying Active Directory for site information and polling the site's domain controllers, a Mac integrated in Active Directory can find not only the closest domain controllers, but also the ones that respond the quickest. Using open Directory, we can implement Group Policies over the Mac clients.

Figure 2: Open Directory

We need to set up Open Directory on a server so that we can bind the Mac clients with it. Steps to set up open directory are mentioned below:

1. Launch Server app and choose the OS X Server from the list, the click continue.
2. Authenticate with your administrative account.
3. Once authenticated, scroll down the list of services and select the Open Directory pane. Adjust the slider to the ON position to get started.
4. A wizard will appear to guide you through the initial setup of the OD. For the first OD in your organization, select the radio button for "Create a new Open Directory Domain" and click next.
5. Next, you'll be prompted to create a Directory Administrator (often referred to as Domain Administrator) account. This will serve to manage directory-related tasks. One can accept the defaults or create your own, just don't forget the credentials since it will be the network equivalent to the local computer's admin account. Click next to create the account.
6. The following step asks for the Organization information and an Administrator email address. This information will be displayed to end-users allowing them to identify the server on the network. Click next to continue.
7. Last, the setup confirmation screen will display all the information entered for review, prior to committing them to create the OD Master. The Master is designated as the first Open Directory server in the group. Additional OD servers in the same group are called Replicas, since directory services function to replicate data across other directory servers in the same group as a form of fault-tolerance in the event a server goes offline. If the settings are correct, click Setup.
8. The configuration process, which includes the creation of the service account, configuring links to services, and directory database may take some time. This depends on the specifications of your server, but typically should not take more than a few minutes on modern nodes.
9. After the setup process has completed, viewing the Open Directory service pane will list all the available directory servers in the group, as well as, their master or replica designation.

Figure 3: Open Directory Configured

Once you have configured open directory successfully, then you need to join the clients to open directory. Steps to join the Mac clients to open directory are listed below:

1. Open System Preferences.
2. Click on Users and Groups.
3. Click the padlock to authenticate in order to make the changes.
4. Once authenticated, select Login Option and click on Edit button.
5. The Network Account Server menu will appear. Click the "+" sign to add a logon server.

Figure 4: Joining Client to Open Directory

6. Locate the desired server from the drop-down list and click OK. (If an SSL message prompt appears, click OK to move on. This warning indicates that there is no valid 3rd-party SSL certificate installed.)
7. The selected server should now appear in the list of logon servers; click Done to complete the task. Now computers will be joined to the Open Directory Domain created in the previous steps and more importantly, allow them to access network resources and services, as they are added.

Open Directory has been officially setup on the server and is now ready to accept network objects joined to the domain. With OD properly configured, management over computer accounts, users and groups, and network-based resources are all possible from the Server app interface.

7. USE OF THIRD PARTY ACTIVE DIRECTORY SOLUTION

Products from Beyond Trust, Centrify, Thursby, and Quest allow policy data to be stored in the Active Directory domain

without requiring IT teams to extend the schema. In general, these solutions allow policies to be set as Group Policy Objects in Active Directory, as is done for Windows clients. Each solution replaces OS X native Active Directory capabilities with each third-party's client-side directory services plug-in. These solutions can also be implemented in enterprise environment to bind Mac with Active Directory and controlling them using Group Policies.

8. CONCLUSION

Large organizations need to manage user identities and access across a variety of services in their environment. Integrating Mac OS X with directory services include multiuser login, enforcing strong authentication policies, managing access to resources and providing a seamless authentication experience. OS X natively integrates into the majority of directory services with ease making itself even more adaptable platform.

Acknowledgment

My thanks to the expert Mr. Laeeq Humam, Consultant, HCL Technologies – IOMC who has contributed in the research work for the development of the paper.

REFERENCES:

[1] Ryan Fass, Mac,world; "Mac support in Active Directory Environment"; March -2007.
[2] Apple Training Series, "Mac OS X Directory Services v10.5" by Arek Dreyer; Jul y – 2008
[3] Wes Miller, Technet; "Interacting with Windows from a Mac Environment" ; December - 2008
[4] Apple Inc; "Mac OS X server Open Directory Administration version 10.6 Snow Leopard; August – 2009
[5] John C. Welch, Macworld; "Macs and Active Directory"; January - 2011
[6] Eric B. Rux, Windows IT Pro; Macworld; "Comparative Review: Mac-to-AD Integration Solutions"; May – 2011
[7] Apple Inc, Apple Technical White Paper "Best Practices for integrating OS X with Active Directory"; February – 2013
[8] Apple Inc, Apple Technical White paper "Mac Management Basics 10.8"; September– 2013
[9] Jesus Vigo, Apple Enterprise; "Integrate Macs into Windows Active Directory Domain"; December – 2013
[10] Centrify; "Mac Management" March 2014
[11] Kevin M. White and Gordon Davisson; Apple Pro Training Series; "OS X Support Essentials 10.9"; 2014
[12] Apple Inc, Apple Technical White Paper "Best Practices for integrating OS X with Active Directory"; December – 2014
[13] Apple Support; Directory Services; February - 2015