

2019

Working Architecture of Active Directory Applications in Libraries

Arumugam J

PSG College of Technology, jacs1986tv1@gmail.com

Balasubramani R

Bharathidasan University, lisbala@gmail.com

Follow this and additional works at: <https://digitalcommons.unl.edu/libphilprac>

Part of the [Library and Information Science Commons](#)

J, Arumugam and R, Balasubramani, "Working Architecture of Active Directory Applications in Libraries" (2019). *Library Philosophy and Practice (e-journal)*. 2238.

<https://digitalcommons.unl.edu/libphilprac/2238>

Working Architecture of Active Directory Applications in Libraries

J Arumugam and R Balasubramani

Librarian, PSG College of Technology, Coimbatore

Assistant Professor, Dept of Library & Information Science, Bharathidasan University, Trichy

ABSTRACT

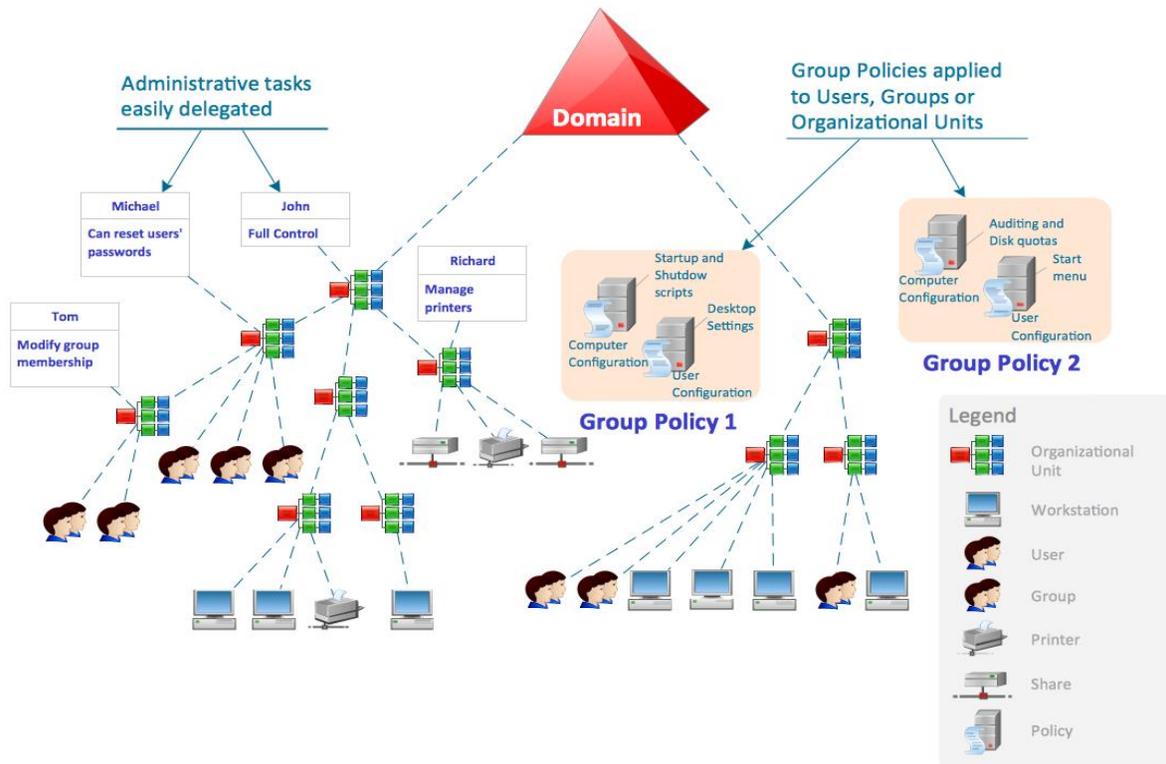
Information Technology revolutionized era offer several tools for creating; organizing; storing and visualization of information in libraries in various perspectives. This paper highlights the application of Active Directory in library and information centers. In this context, Active Directory is an extensible directory service that enables managing and storing the detailed information about each network resources efficiently and also used to record the user access count as well as the duration of time spent by the user in the library. It is also used to maintain the institutional User restriction policies in the Server-Client architecture in libraries. This paper explains the steps to deploy the User access and reporting modules, credentials to the user by using the Windows Active Directory and also explores the technical aspect of working architecture, application and its limitation in the libraries.

Keywords:- Active Directory, Library and Information Centers, Windows Active Directory

INTRODUCTION

Windows active directory server has information about all the objects of users, computers, and resources like printers, shared files or folders connected in an organizations network. Active directory tool facilitates to arrange, store information, provides access and permission based on that information. Active Directory networks are arranged in four categories that are forests, domains, organizational units and sites. The forests are collection of every object based on its attributes and attribute syntax. Domain is a collection of computers that share a common set of policies for the name of members. Organizational units where domains can be grouped, creating a hierarchy and the structure of active directory. Site is a physical grouping which is independent of the domain and organizational unit.

Active Directory is useful for organizing network systems in a hierarchical structure for creating the infrastructure and storing information about the objects like users, computers, printers and share folders. Active directory reduces costs on the infrastructure and maintenance.



Active Directory is highly secure and possible to have layered security, which is having policies and permissions for security at different levels. It is easy, efficient search mechanism to locate an object that can be located anywhere physically access the domain or network's resources.

NEED OF ACTIVE DIRECTORY SERVICES

Active directory can be used in the following various set up in order to enhance the value of the organizational security.

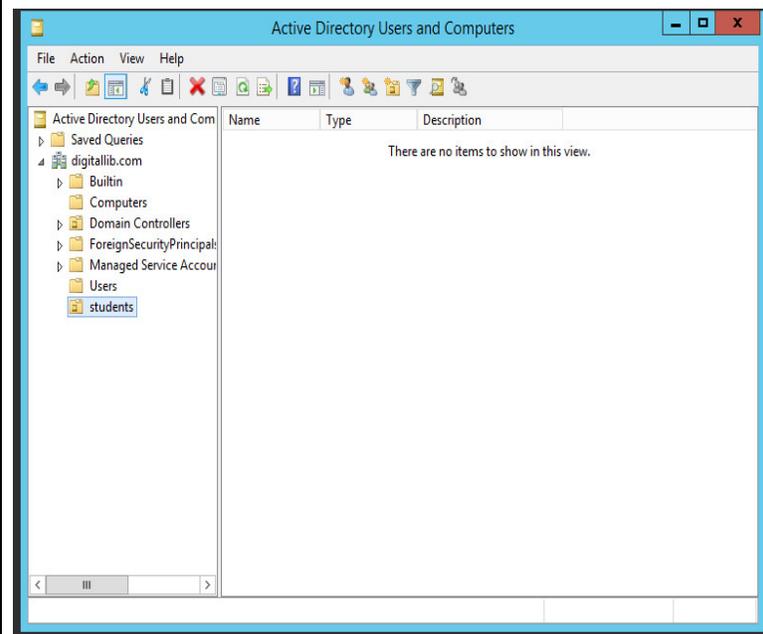
- ❖ Any organization that has a network setup
- ❖ Organization which requires 24*7 uptime
- ❖ Any organization where the number of users, computers or resources will keep changing
- ❖ Any organization where information or data security is vital
- ❖ Any organization that operates in multiple locations

WORKING ARCHITECTURE

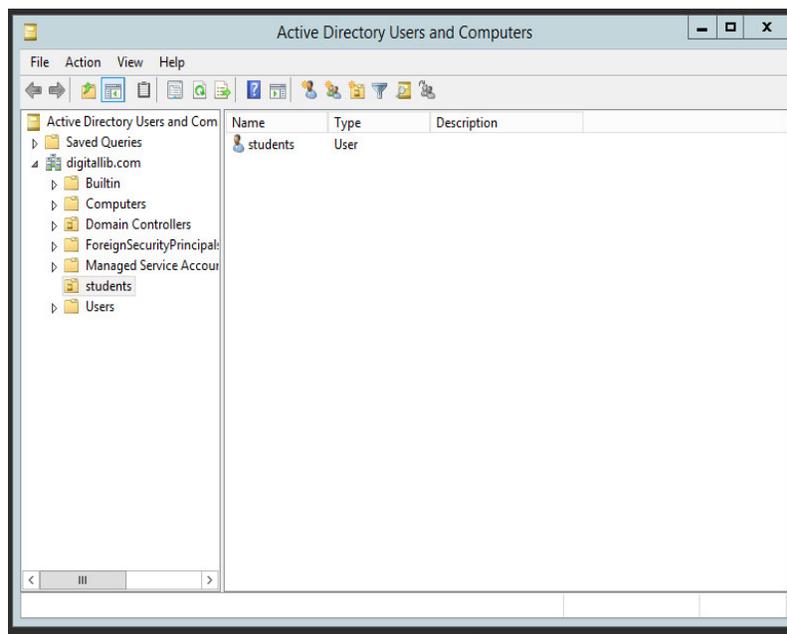
The Active Directory is properly installed, configured and patched with the latest updates and service packs as released by Microsoft. Correct configuration requires the Access Control Lists (ACLs), that are used to control access to objects in the Active Directory, and to set up minimum privileges to the users. The guidelines discussed in this paper will be effective only if the Active Directory is properly installed, configured and patched with the latest updates and service packs as released by Microsoft. The working concept of Active directory as follows.

- ❖ Installation of Windows Server and Active Directory
- ❖ Creation of Category/ Organization Unit
- ❖ Addition of User
- ❖ Setting up Group Policy Management Tool
- ❖ Policy creation of Category of Organization Unit
- ❖ Logon/ Logout Script for User Activity

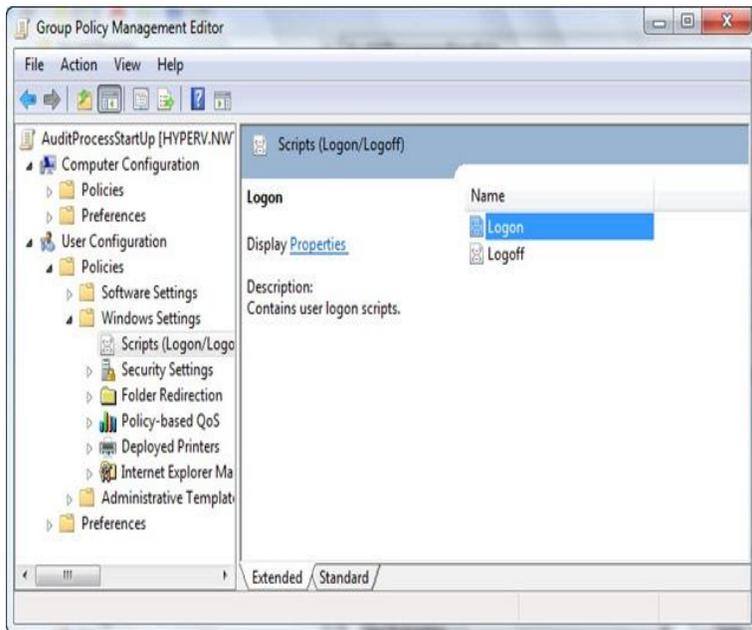
Step 1: Homepage of Active Directory



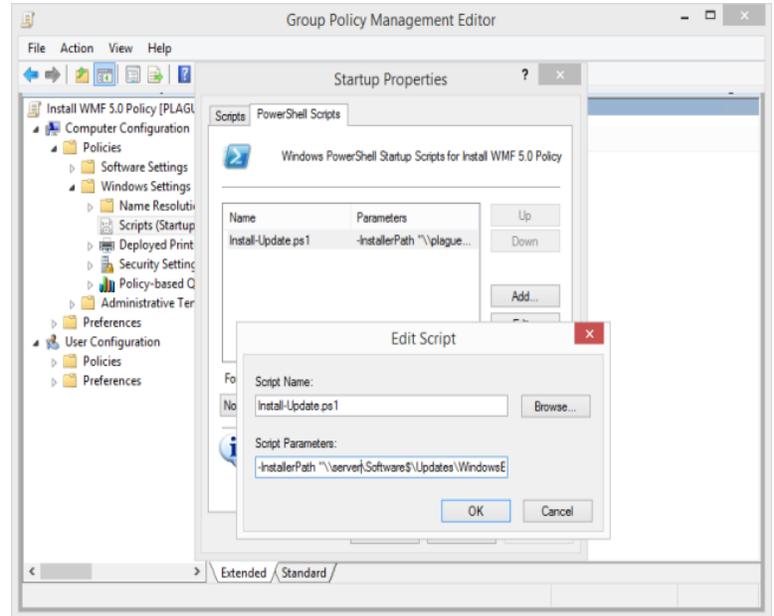
Step 2: Creation of User in the Active Directory



Step 3: Group Policy Management Editor



Step 4: Group Policy Management Script Run



Step 5: Script for Group Policy

@ECHO OFF

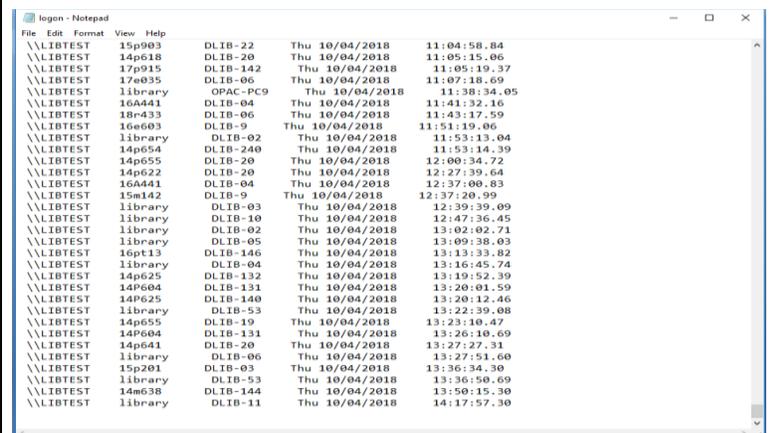
Echo %logonserver% %username% %computername%

%date% %time% >> \\ IP Address for Share Folder

\Log\logon.txt

exit

Step 6: User Log in/ Out Output Screen



APPLICATION OF ACTIVE DIRECTORY IN LIBRARIES

Active Directory is a core service holding user, server account details and security information. Access to Active Directory needs to be well controlled and protected; otherwise an attacker could severely impair the correct functioning of both the Web application and the back office by successfully launching an attack on Active Directory. Web application builders need to understand the vulnerabilities of Active Directory and the threats that can potentially exploit these vulnerabilities.

The concept of active directory is used mainly in the libraries for the purpose of creating the user profile of the library and also to monitor the activities of the users in the digital library. It also facilitates to analyze the usage of digital library by the different category of the user community. It also develops a proper system to monitor the activities of the user as well as the statistical analysis of the user's activity.

THREATS AND COUNTERMEASURES

There are certain threats need to be taken care of while using the active directory applications. Spoofing can take one of two forms. Either an attacker attempts to spoof a user or an attacker attempts to spoof the Active Directory. The attacker captures or guesses a user's credentials and then masquerades as the user when accessing the Active Directory. Spoofing a user can be aided by vulnerabilities in the network, vulnerabilities in the Active Directory Information Base and vulnerabilities in the Application Server. An attacker can sniff the network to obtain user account names and passwords, or access the Active Directory to retrieve valid user account names and then find the password by either a dictionary attack or modifying the password attribute in the directory.

Tampering is known as an attacker tries to modify directory data either in transit to the client, or whilst it is stored in the AD server. This can be due to vulnerabilities in the network, which are vulnerabilities in the Active Directory Information Base or vulnerabilities in the Application Server.

Repudiation is another threat when users deny that they have performed specific actions or transactions. Keeping adequate audit trails will provide evidence of who did what and will help to counteract this type of threat.

Information disclosure occurs when a user gains read access to information that anyone is not supposed to have access to. This can be due to vulnerabilities in the network, vulnerabilities in the Active Directory or vulnerabilities in the Application Server.

Denial of service attack, the attacker denies access to the AD server for normal users. This can be aided by vulnerabilities in the Active Directory server and vulnerabilities in the Application Server.

There are certain counter measures for the application of active directory. Ensure that the Access Control Lists in the AD server are correctly configured to give minimum privileges to clients and also limit the number and scope of directory operations that the Application Server sends to the AD server on behalf of the client.

CONCLUSION

Implementation of active directory in the library facilitates to analyze the nature of the user as well as the utilization of the resources in the library. It helps to authenticate the user from the unwanted URLs / Information. Active Directory ensures the resource usage and the authority of usage by the users where as the unwanted sites can be white listed and monitored by using this concept. The designing policies for the user and the technical implementation may require software knowledge but it can be manageable and easily understandable by the library professionals. The hurdles of high cost implementation can be redesigned by adopting these kind of techniques in the libraries may throw lights on the libraries and library professionals.

References

1. Kille, S et.al. (1998) "Using Domains in LDAP/X.500 Distinguished Names", RFC 2247.
2. MSDN Library (2003) "Creating More Efficient Microsoft Active Directory-Enabled Applications." <http://msdn.microsoft.com/library/enus/dnactdir/html/efficientadapps.asp?frame=true>

3. MSDN Library (2003) "Improving web application security: Threats and Countermeasures"
<http://msdn.microsoft.com/library/default.asp?url=/library/enus/dnnetsec/html/ThreatCounter.asp>
4. Wahl, M., Alverstrand, H., Hodges, J., Morgan, R. (2000) "Authentication Methods for LDAP", RFC 2829, May 2000