ISSN 2278-3091
Volume 9, No.1, January – February 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse14912020.pdf
https://doi.org/10.30534/ijatcse/2020/14912020

Conducting Empirical Research Study: How to Effectively and Securely Use the Vital Features of the Active Directory Network Server

Dr. Omar Khattab[1], Hadeel Alzayed[2], Anfal Almutairi[3], Zainab Yousef[4]
[1]Assistant Professor, Dept. of Computer Science & Engineering
[2]BEng Student, Computer Engineering Program
[3]BEng Student, Computer Engineering Program
[4]BEng Student, Computer Engineering Program
Kuwait College of Science and Technology (KCST), Kuwait

ABSTRACT

The Active Directory (AD) is a network operating system which effectively stores and manages companies' resources such as employees (e.g., users and groups), devices (e.g., computers, servers and printers), applications and files. In this paper, a recent research work about the AD has been considered, where it confined in analyzing one company which didn't implement AD. Therefore, this paper has thoroughly analyzed various companies whether they use AD or not (AD vs. non-AD), in order to come up with an optimized practice solution in using and utilizing the vital features of AD.

Key words: Active Directory (AD), Microsoft's Network Operating System, Windows Server, Group Policy

1. INTRODUCTION

Recently most of the companies have relied on the Active Directory (AD) as a central database for managing their available resources, which exist in the network such as users, computers and groups [1], as shown in the Figure 1.

The AD has several vital features which effectively and securely help companies in improving their performance of duties and tasks. Some of its main features are mentioned below [1]:

- It makes the management of network resources and security policy simpler and easier.
- It manages all network resources from one place without needing to change location.
- It has the ability to expand with the organization. It does not limit the company rather it is very adaptable to the changes of the company.
- Login security feature is improved compared to another directory service.

This paper has thoroughly analyzed various companies in Kuwait whether they use AD or not (AD vs. non-AD), in order to come up with an optimized practice solution in using and utilizing the vital features of AD.

The rest of the paper is organized as follows: Section 2 presents a related work of AD. Section 3 presents a comprehensive analysis of the AD vs. non-AD. Section 4 presents the proposed AD design. Finally, a conclusion work is given in section 5.

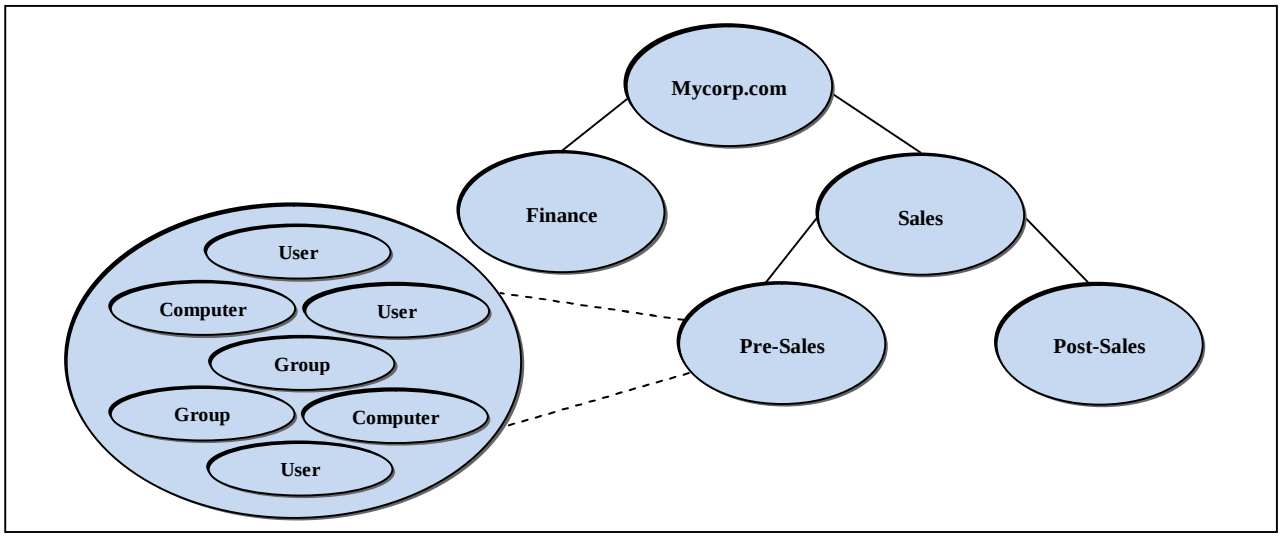

Figure 1: A Hierarchy of Objects in the AD [2]

2. A RELATED WORK OF AD

This paper considers a recent research work about the AD which was applied on a Saudi company. In [1], the authors analyzed a company which didn't implement AD. They concluded that the AD must be implemented in all company's departments due to its critical role of managing their resources and keeping their system secure.

3. A COMPREHENSIVE ANALYSIS OF THE AD VS. NON-AD

In [1], we have observed that the research work was only based on one company which didn't implement AD, as well as no comprehensive empirical work was provided in this respect. We have thoroughly analyzed various companies in Kuwait in order to recognize the nature of their business and to get a better understanding about their system. This helps in protecting it against any potential issue that they might experience directly or indirectly (hidden vulnerabilities). We have divided our survey into two main parts: the first, for the companies which already use AD while the second, for the companies which don't use it (non-AD). In our survey, we have concentrated on the most six common security issues of AD [1]. This is shown in the Figure 2.

Although the AD is prevalent option between companies, a few of them know how to use it effectively and securely [1]. Besides, both of IPv4 and IPv6 are still vulnerable to the security threats [3].

As shown in the Table 1, most of the companies experience from a common issue: "password length", which is less than 20 characters. It could be easily guessed and exploited to elevate credentials [4].

As for "version of windows server", there are some companies still don't use the latest version of windows server 2019. This results in losing new vital features of AD. Windows server 2019 supports the following new features [5]:

- Enhanced security capabilities
- Faster innovation for applications
- Unique hybrid capabilities with Azure
- Unprecedented hyper-converged infrastructure

A fair comparison between windows server versions (windows server 2008, windows server 2012, windows server 2016 and windows server 2019) is available in [5].

For "using GPP to handle credentials", there is one company manages its credentials using GPP. This is one of the most common credential theft scenarios [4].

In terms of "number of employees and willing to use/improve the network", there are two companies with a huge number of employees show their interest of using AD, in order to improve their daily tasks.

4. THE PROPOSED AD DESIGN

It has been noticed from the section 3 that that most of companies still experience some vulnerabilities as they don't have enough knowledge about them: password length, version of windows server and GPP, this results in elevating credentials, losing new vital features of AD and being vulnerable to the most common credential theft scenarios; respectively. We therefore provide an optimized practice solution in using and utilizing the features of AD, as shown in the Table 2.

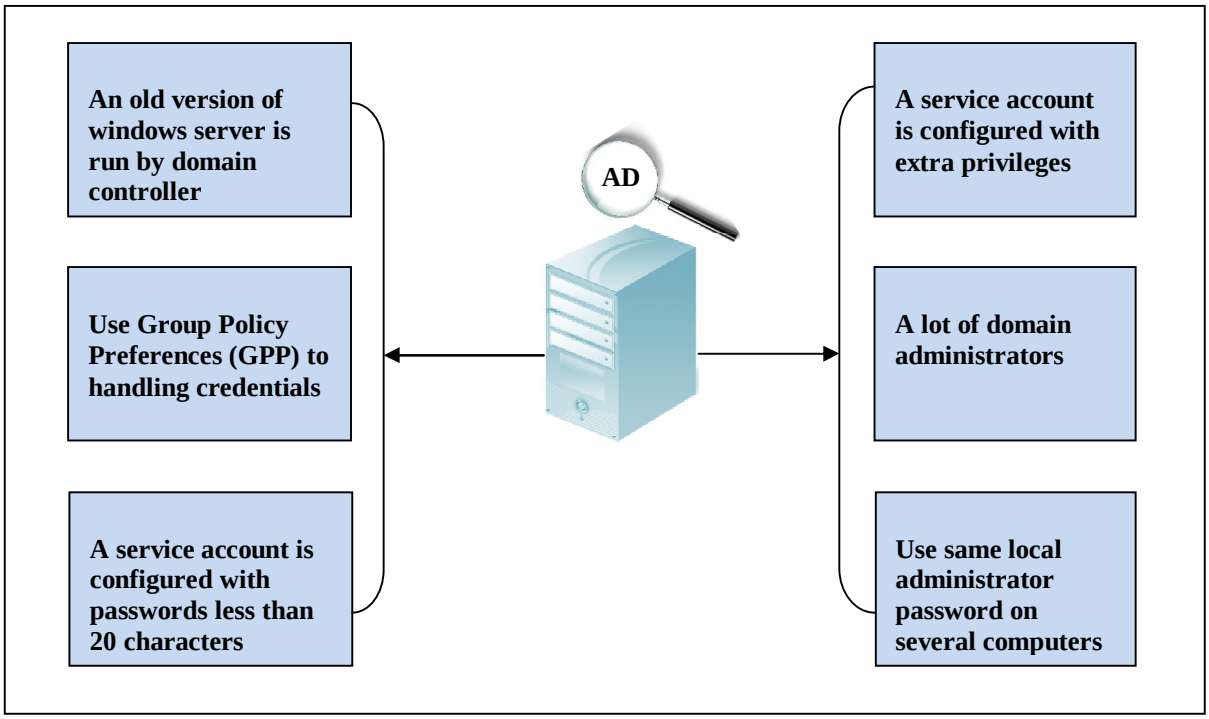

Figure 2: The Most Six Common Security Issues of AD

Table 1: Comparison of AD vs. Non-AD

	#	1	2	3	4	5
	The nature of company	**Flights and hotels online booking**	**Restaurant**	**Utility services**	**Information and communication technology**	**IT solutions**
	The number of employees	> 100	380	> 23000	200	800
	Implement AD			✓	✓	✓
Security Issues Of AD	**A lot of domain administrators**					
	A service account is configured with passwords less than 20 characters			✓	✓	✓
	Using GPP to handling credential				✓	
	An old version of windows server is run by domain controller				Windows Server 2016	Windows Server 2016
	Same local administrator password on several computers					
	A service account is configured with extra privileges					
	Willing to use/improve the network	✓	✓	✓	✓	✓

Table 2: Addressing Security Issues of AD

#	Issue	How to address it
1	**Extra privileges**	Configure each service account with the required rights [4]
2	**A lot of domain administrators**	Configure the AD administrator to be sole responsible for privileges domain [4]
3	**Local administrator password**	Configure a unique credential for each local administrator account on each computer [4]
4	**Version of windows server**	Install the latest version of windows server [4]
5	**GPP**	Avoid using GPP to manage credentials [4]
6	**The password length**	Configure a password length for a service account with more than 20 characters [4]

5. CONCLUSION

This paper has presented a recent research work about the AD. It obviously confined in analyzing one company which didn't implement AD. Therefore, we have thoroughly analyzed various companies: AD vs. non-AD. It has been noticed that most of these companies still experience some vulnerabilities as they don't have enough knowledge about them: password length, version of windows server and GPP, this results in elevating credentials, losing new vital features of AD and being vulnerable to the most common credential theft scenarios; respectively. In the future work, we plan to implement the AD taking into account the all its security issues.

REFERENCES

1. A. Binduf, H. Alamoudi, H. Balahmar, S. Alshamrani, H. Al-Omar and N. Nagy, **Active Directory and Related Aspects of Security**, Saudi Computer Society National Computer Conference (NCC), 25-26 Apr 2018, pp. 4474-4479.
   https://doi.org/10.1109/NCG.2018.8593188
2. B. Desmond, J. Richards, R. Allen and A. Lowe-Norris, **Active Directory**, 5 th ed. Sebastopol, USA.: O'Reilly Media, Inc., 2013, pp. 1-712.
3. O.Khattab, **A Comprehensive Survey on Vertical Handover Security Attacks during Execution Phase**, International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, no. 5, Sep- Oct 2019, pp. 1965-1968.
   https://doi.org/10.30534/ijatcse/2019/20852019
4. S. Metcalf, **The Most Common Active Directory Security Issues and What You Can Do to Fix Them – Active Directory Security**. Retrieved 13 Jan 2020 from: https://adsecurity.org/?p=1684.
5. **Compare features in Windows Server versions**. Microsoft. Retrieved 13 Jan, 2020, from https://www.microsoft.com/en-us/cloud-platform/windows-server-comparison.