APPLICATION OF DOMAIN CONTROLLER TECHNOLOGY IN USER COMPUTER SECURITY

Nguyen Quoc Tuan, Tran Thi Thu Phuong

Hanoi Metropolitan University

Abstract: *Recent attacks, infections, and malicious code are mostly exploited by hackers as a potential vulnerability on unsecured user computers. The issue for administrators is how to protect hundreds of computers within the organization from such insecurity. One technology that is not new for Microsoft but is rarely applied by Vietnamese companies is Domain Controller. The Domain Controller model enables centralized management of objects participating in the network, aimed at: authenticating properly (computer, user); establishing security policies; deploying software, vulnerability patches remotely quickly.*

Keywords: *Secure, domain, domain Controller.*

Received 5 Janurary 2023

Revised and accepted for publication 24 July 2023

Contact author: Nguyen Quoc Tuan; Email: nqtuan@hnmu.edu.vn

1. INTRODUCTION

Domain (domain or region) is an important concept in the Windows network, a domain is a collection of user accounts and computer accounts that are grouped together for centralized management, and management is for domain controllers to make resource exploitation easier and more secure. In peer-to-peer networks, workstations function as stand-alone systems, and user accounts, or local user accounts that cannot control network resources, are only accessible and exploited on the local machine. So Domain is a discovery that is made to solve the difficulties that the peer-to-peer network has not, it has the task of centralizing the user accounts and all management and policy setting work is through this domain controller. This makes administration easier and allows users to log in from any computer that joins the network.

Domain provides authentication services to identify the right objects (user, computer) when these objects join the network. That is, when a user logs in to the network, will a domain controller check the validity of the username and password they enter is correct and matches the data stored on the server?

Resources on the Windows network are protected by Access Control Lists- ACL (Access Control List). An ACL is a list that specifies who has the authority to do what. When a user attempts to access a resource, they give their identity to the server that contains the resource. The server will check to make sure that this user identity has been verified, then cross-reference to ACL to see what the user has permission to do?

On the other hand, through the Active Directory Database, administrators can also deploy applications to workstations automatically and quickly. The role of domain controller is very important in an Active Directory infrastructure because it holds the credentials for all authorized users in the domain system. It can also be used by domain administrators to manage security settings on all domain member machines.

2. RELATED CONCEPTS

2.1. Domain

Domain is actually a description of a system, collection of users, applications, data servers or any other type of resource that is of interest and used by an enterprise. They will be managed according to some common set of rules with distinct characteristics. In a Windows environment, domain is a set of resources (set of user accounts, computer accounts, ...) grouped together for centralized management.

2.2. Domain Controller

A domain controller is the server responsible for managing network and identity security requests. It acts as a gatekeeper and authenticates whether the user is authorized to access the IT resources in the domain. The Microsoft Windows Active Directory Server hierarchically organizes and protects user information, business-critical data, and IT devices operating on the network [1]. The domain controller is classified into 2 types– PDC and BDC:

Primary Domain Controller – PDC: Primary Domain Controller is a domain scroller of Microsoft Windows NT. This domain controller contains a master copy of the Security Account Manager (SAM) database. Each Windows NT domain has only one PDC. This PDC is periodically synchronized directory, in order to replicate its own database directory. From there you can backup the domain controller in the domain. The PDC must be the first computer that installed inside the domain and identifies the domain.

Backup Domain Controller – BDC: To manage access to network resources, Windows NT requires a backup domain controller (BDC). The BDC is responsible for maintaining a read-only copy of the user account database. Also verify logins from user. The read-only copy of the database is synchronized with the primary domain controllers. In addition, the BDC can also be upgraded to a PDC if the network is busy or the PDC fails. Microsoft recommends that users only upgrade to PDC when the PDC is active. Then, if you downgrade to BDC again, the data will not be lost.

2.3. Active Directory

Active Directory is a directory management service that can contain information about computers in the network, network users, printers, applications on the network... By storing information in a central directory, all of these resources can be shared with everyone at all times. [2]. The Domain model is a hierarchical directory architecture of resources – Active Directory – and is used by all systems that are members of the Domain. These systems can use the user, group, and computer accounts in the folder to secure their resources. The Active Directory therefore serves as an identity storage center, providing a trusted list indicating “who is who” in the Domain. [3].

Active Directory itself serves as a database, which contains a list of supporting components, including transaction logs and sysvol, which contains information about login scenarios and group policies. Active Directory uses LDAP (Lightweight Directory Access Protocol), Kerberos security protocol, data synchronization cycles, and FRS (File Replication Service) file synchronization services.

There are some common objects are used in Active Driectory. The root object that contains other objects is Domain. To create logical groups such as computers, users, groups, use Organizational Unit. User represents a network user and performs the function as data for identification and authentication. For log in to the Domain, computer represents a computer in the network and provides the necessary computer account. Group: a container object that represents a logical group of users, computers or other groups, independently in the structure of Active Directory. Groups can contain objects from OUs and Domains. In order to share folder in a Windows computer, shared folder provides Active Directory-based access. Finally, Printer provides Active Directory-based n Each Active Directory object contains a set of attributes, which are information about the object. For example, the user object will have attributes that describe the account name, password, address, phone number... A group object will have properties that indicate the list of users who are members of that group…

Besides purely informative properties, objects also have properties that perform administrative functions, such as an Access Control List that specifies who is allowed to access the object network access to a printer in a Windows computer.

2.4. Group Policy

Due to the way the settings from the parent level to the child level are inherited, the administrator can use the OUs to collect objects that need the same configuration. Configuration settings that are applied to each Windows computer can also be managed centrally using an Active Directory feature called Group Policy.

Group policies allow defining security settings, software deployment, operating system configuration, and how applications work on a computer without having to do it directly on the computer to be set up.

The setting of configuration options on a special object of the Active Directory called the Group Policy Object (GPO) then connects these GPOs to objects in the Active Directory that contain the computers or users that want to apply them.

3. IMPLEMENT DOMAIN IN HANOI METROPOLITAN UNIVERSITY

3.1. Deployment model

The centralized authentication model via Active Directory allows Hanoi Metropolitan University to solve the problem of having to use multiple user accounts for different needs such as logging in to access resources, using email. This model deals with identity, decentralization, authentication, and centralized management of all resources in the system (users, databases, etc.). Besides, this model also provides redundancy as well as automatic failover when two or more domain controllers perform the conversion on the domain.

In Active Directory, users can easily access all the resources on the network with just a single login. However, users can be assured because the security mechanism is relatively strong and can easily identify each user as well as restrict the access to resources of some objects. Active directories, in particular, can enable the downgrade of domain controllers and member servers easily and are protected from Group Policies.

This is a flexible protection system, allowing management to become easier and delegating responsibility to managers.

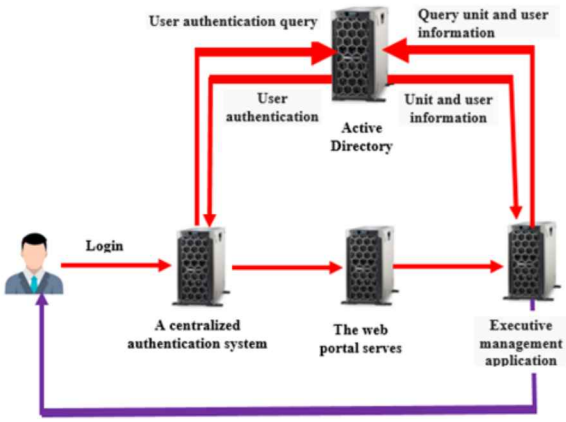

Figure 1. Centralized Authentication Model via Active Directory

AD (Active Directory) serves as the user database on the network, allowing user validity checks and storing information about that user and other resources on the network.

A centralized authentication system is an intermediate application that acts as a service, checking the validity and user access to applications and resources on the network.

The web portal serves as a centralized and unified gateway for all applications and resources on the network.

3.2. Workstation security policies

Set the network resource access rights according to the task function for each target group.

Business data mining workstations are only allowed to use the application, not to install any other software.

Remote implementation of application software for workstations.

Remotely deploy anti-virus software to workstations, and perform remote scanning.

Control the connection status of the workstations.

Controls the user's login status and resource usage.

3.3. Results

Domain is a concept that is not new but it is less implemented in Vietnam, because in addition to the advantages of management and security, this model also causes many troubles and discomforts for users (because the policies are controlled by domain controller).

However, the implementation of testing on some Hanoi Metropolitan University network areas has shown the results and advantages that this model brings:

- Joining Domain and implementing security policies for workstations when participating in the network has greatly limited the risk of spreading viruses from the network, insecure devices into the Group's critical information applications.

- Joining Domain and deploying remote applications to workstations is done quickly.

- Control and properly assign permissions to different target groups who are allowed to access resources on the network.

Advantages and disadvantages of domain controller

The use of domain controllers has advantages and disadvantages. The first advantage is Control Active Directory administration privileges and limit domain user accounts. Before granting access rights to sensitive files, the domain controller ensures every computer connected to a network is authorized. User accounts are reviewed carefully and provided administrative privileges and access to only those who need them to perform their job functions. It also ensures user accounts are protected with robust passwords. Avoiding “operator error” data breaches is the second advantages. As insecure passwords are one of the leading causes of data breaches, the data controller provides network-wide security policies, such as those that require users to set a unique and robust password. Another good point is the network central management. Due to the managing and configuring devices individually is a time-consuming task, a domain controller can save cost and time to set login and security parameters for devices from a centralized server. In addition, the network printers are automatically installed as soon as they join the domain. Using domain controller allows sharing resources, it enable sharing of resources as all the devices are connected centrally. The login-specific access privileges and access any computer or device can be set, this helps reduce the cost required to purchase new printers, computers, and more. And the final advantage is the permission sharing of resources. Because it has set security controls to prevent user accounts from accessing your network with too many failed login attempts, so It can disable user accounts immediately when an employee leaves an organization, require login credentials for locked screens, and restrict USB access based on user permissions and access rights.

However, there are some disadvantages in using domain controller. Because it has complex structure, as a result, that be difficult for a single user to understand. To set up a domain controller, a proper planning required for the network. As ensuring security policies and administrative privileges are up to date, it requires regular monitoring and management. And the final is the entire network is dependent on the domain controller’s uptime.

4. CONCLUSION

Domain is a very effective centralized management model on the Window environment, which reduces the workload for computer network administrators in matters related to management and security:

- Authenticate the right objects (user, computer) through the database stored on the Active Directory. On the other hand, because user account profile management is centralized on the server, users can access from any computer on the network (with join domain) to work with unchanged permissions and interface.

- Set security policies through ACL such as: access rights, access time, application installation rights computers, access to resources on the network…

- Deploy applications remotely to workstations quickly such as application software, antivirus software, patches for the system.

REFERENCES

1. "What Is a Domain Controller?" (2022). https://www.solarwinds.com/resources/it-glossary/domain-controller.
2. P. Gkotsis (2021). *Creating a Windows Active Directory Lab and Performing Simulated Attacks*. University of Piraeus, Piraeus, Greece.
3. R. Allen (2003). *Active Directory Cookbook.*

ỨNG DỤNG CÔNG NGHỆ DOMAIN CONTROLLER TRONG BẢO MẬT MÁY TÍNH NGƯỜI DÙNG

Tóm tắt: *Các cuộc tấn công, lây nhiễm mã độc hầu hết do tin tặc lợi dụng các lỗ hổng tiềm ẩn trên máy tính người dùng không được bảo mật. Vì vậy, người quản trị cần sử dụng một công cụ nào đó để bảo vệ hàng trăm máy tính người dùng trong tổ chức của mình để tránh các nguy cơ mất an ninh an toàn đó. Một công nghệ không hề mới của Microsoft nhưng ít được các doanh nghiệp Việt Nam quan tâm đó là Domain Controller. Mô hình Domain Controller cho phép quản lý tập trung các đối tượng tham gia vào mạng, nhằm mục đích: xác thực chính xác đối tượng; thiết lập các chính sách về bảo mật; triển khai phần mềm, bản vá lỗ hổng từ xa một cách nhanh chóng.*

Từ khóa: *Bảo mật, domain, domain controller.*