Active Directory and Secure Authentication/ Authorization

Wesley Faxlanger

School of Cybersecurity

CYSE:608 Cyber War

Dr. Malik A. Gladden

20 September 2026

Active Directory and Secure Authentication/ Authorization

Active Directory Domain Services (AD DS) is defined by Microsoft as "a directory service that provides the methods for storing directory data and making this data available to network users and administrators" (Microsoft, February 3, 2025). AD DS is a hierarchical structure that stores information about objects on a network, AD DS also provides integrated security measures such as sign-in authentication and access controls (Microsoft, February 3, 2025). Ideally, administrators can use one set of login credentials to manage and access resources, regardless of where they are on the network. Key components of AD DS include forests, domains, organizational units (OUs), domain controllers, the schema, the global catalog, and replication. The forest sits at the highest level of the hierarchy, while domains divide directory data into administrative and replication boundaries. OUs organize users, devices, and groups, allowing administrators to apply Group Policies or delegate administrative controls. Domain controllers are responsible for storing directory information and provide authentication, while the global catalog helps users and applications locate objects across the forest (Microsoft, May 12, 2025).

Authentication and authorization are two of Active Directory's most important functions. Authentication verifies the identity of a user or computer attempting to sign in, while authorization is responsible for determining what permissions the individual or device has been granted. In short, this means that authentication ensures that something is what it says it is, while authorization ensures that a verified user is only granted access necessary to perform their task. Domain controllers are responsible for providing authentication and information related to authorization, such as group memberships, that can be used to control access to network resources (Microsoft, May 12, 2025). Authentication is commonly achieved in Active Directory

using Kerberos, although sometimes legacy software such as NTLM may be used. Access control lists, security groups, and Group Policy are then utilized by administrators to manage permissions and security settings throughout the network.

Unfortunately, Active Directory possesses several significant security vulnerabilities as it is a centralized system. If a bad actor obtains privileged credentials or compromises a domain controller, the attacker could gain potentially unrestricted access to sensitive systems and information throughout the organization. Microsoft acknowledges that credential theft, lack of effective access controls, mismanagement of privileged accounts, and poorly protected domain controllers are major risks for organizations using this service (Microsoft, May 12, 2025). This is where the principle of least privilege and zero trust comes into play. Strictly limiting membership to privileged groups and utilizing separate and specific admin accounts is critical to ensuring an organization remains secure. Ultimately, using privileged admin accounts for daily tasks is a major security risk. Ultimately, the devices hosting the admin accounts need to be secure, and multi-factor authentication should be utilized to minimize the risk of a breach. Additional protections are necessary for authentication traffic and directory communications.

In conclusion, Active Directory security relies on a combination of proper security controls and proper administration practices. OU design, Group Policy, secure authentication, least-privilege access, protection of privileged accounts, LDAP signing, monitoring, and ensuring that patches and updates are pushed immediately are all critical aspects of ensuring that unauthorized access does not occur. When best practices are utilized, Active Directory provides centralized, scalable authentication and authorization in a manner that does not negatively impact the availability or security of an organizations resources.

References

Microsoft. (2025, March 11). *Active Directory Domain Services overview*. Microsoft. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Microsoft. (2023, November 10). *Best Practices for Securing Active Directory*. Learn.Microsoft.Com. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

Microsoft. (2025, May 12). *Understanding the Active Directory Logical Model*. Learn.Microsoft.Com. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-the-active-directory-logical-model

Microsoft. (2026, January 16). *LDAP signing for Active Directory Domain Services on Windows Server*. Microsoft.Com. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/ldap-signing