# Active Directory

Devin P. Johnson

Old Dominion University: School of Cybersecurity

CYSE 608: Windows Systems for Cybersecurity

Dr. Malik A. Gladden

March 13, 2026

## Introduction

Active Directory Domain Services is Microsoft's directory service for Windows domains. It stores identity and resource data and makes that data available to authorized users and administrators. It also acts as the control plane for authentication and access decisions across domain-joined systems (Microsoft, 2025a).

## Key components and functions of Active Directory

A central component of AD is the directory data store. This holds objects such as user accounts, computer accounts, groups, and shared resources. The directory is organized logically and hierarchically, which supports enterprise administration and delegation (Microsoft, 2025a). AD is governed by a schema, which defines object classes and attributes. The schema is critical because it standardizes what can exist in the directory and how objects are described (Microsoft, 2025a).

Active Directory is deployed through domain controllers. DCs host AD DS and provide authentication and directory services to clients. AD also includes a global catalog, which contains information about every object in the directory and supports searches across domains (Microsoft, 2025a). To maintain consistency, AD uses replication, which distributes directory changes across domain controllers. Each domain controller maintains an up-to-date copy of directory data for its domain (Microsoft, 2025a). Operationally, replication enables resilience and reduces dependence on any single server.

From an architecture standpoint, AD is structured into domains and forests. Domains provide administrative and security boundaries for objects. Forests provide the top-level boundary for directory trust and schema (Microsoft, 2025a). Within domains, organizations use organizational units to group objects and delegate administration. OUs also support policy targeting through Group Policy, which enforces configuration settings and security controls (Microsoft, 2025a).

AD authentication and authorization are closely linked. For authentication, Kerberos is the preferred mechanism in AD environments, while NTLM remains supported for certain legacy scenarios (Microsoft, 2025b). For authorization, AD relies on group membership and access control mechanisms tied to directory objects and resources. This combination enables centralized identity management and consistent access decisions across systems (Microsoft, 2025a).

## Primary security risks and mitigation strategies

AD is the identity backbone for many Windows enterprises. Compromise often results in broad control of systems and data. One major risk is misconfiguration and weak operational hygiene, including incomplete patching and insecure settings. Microsoft identifies misconfiguration and incomplete patching among the common weaknesses observed in real AD deployments (Microsoft, 2025c). These issues increase exposure to credential theft, privilege escalation, and lateral movement.

A second major risk is credential abuse of Kerberos. For example, attackers can exploit service account ticketing to extract material used for offline password cracking, which can accelerate privilege escalation if service accounts have weak passwords or excessive permissions (Microsoft, 2024). A related risk is the Golden Ticket technique, in which an adversary with the KRBTGT password hash can forge Kerberos ticket-granting tickets and generate authentication material for any account in the domain (MITRE ATT&CK, 2025). This threat is especially severe because it can persist and bypass normal access pathways.

A third risk is legacy authentication exposure. NTLM persists for compatibility but expands attack surface in mixed or older environments. Microsoft notes Kerberos is preferred, yet NTLM may still be used in workgroup scenarios or by specific applications (Microsoft, 2025b). In practice, continued NTLM reliance can increase the likelihood of credential relay and other downgrade risks.

Mitigation should prioritize controls that harden identity, reduce privilege, and improve detection. First, organizations should enforce least privilege and reduce membership in highly privileged groups. Microsoft's AD security guidance emphasizes reducing exposed attack surface and protecting weak points commonly used by attackers (Microsoft, 2025c). Second, administrators should strengthen service accounts using long, complex passwords or managed service account patterns (Microsoft, 2024). Third, organizations should implement monitoring and rapid response procedures for suspected domain compromise. Ticket forgery techniques can enable wide access if not detected quickly (MITRE ATT&CK, 2025).

Finally, strong authentication policy is essential for administrative accounts. NIST's digital identity guidelines stress selecting appropriate authenticator assurance levels and using stronger authenticators to reduce the impact of credential compromise (NIST, 2017). Applied to AD, this supports adopting phishing resistant MFA for privileged workflows, limiting standing admin access, and requiring controlled admin workstations and processes for domain administration (NIST, 2017; Microsoft, 2025c).

**References**


Microsoft. (2024, October 11). *Microsoft's guidance to help mitigate Kerberoasting*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2024/10/11/microsofts-guidance-to-help-mitigate-kerberoasting/

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

Microsoft. (2025b, April 18). *NTLM overview*. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/security/kerberos/ntlm-overview

Microsoft. (2025c, May 21). *Best practices for securing Active Directory*. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

National Institute of Standards and Technology. (2017). *Digital identity guidelines: Authentication and lifecycle management (SP 800-63B)*. https://pages.nist.gov/800-63-3/sp800-63b.html

MITRE ATT&CK. (2025, October 24). *Steal or forge Kerberos tickets: Golden Ticket (T1558.001)*. https://attack.mitre.org/techniques/T1558/001/