BRYANT WATKINS

CYSE 608 | Dr. Gladden

Active Directory Research

3/4/26

Prompt: "What are the key components and functions of Active Directory? What are the primary security risks and mitigation strategies related to the management of secure authentication and authorization processes?"

Active Directory Key Components & Functions

Active Directory is a powerful tool and platform that is composed of numerous components and functions. Active Directory is composed of five main components - Active Directory Domain Services, Lightweight Directory Services, Certificate Services, Federation Services, and Rights Management Services. These components work together to form the foundation of Active Directory's functions. Active Directory is a versatile asset capable of managing user accounts, securing information systems, and managing devices within an organization.

Active Directory Domain Services allows administrators to configure policies, store data, and authenticate users. The integration of DNS services and consolidation of account management are key features of Active Directory Domain Services. Lightweight Directory Services is, as the name implies, lightweight. Lightweight Directory Services is ideal for Active Directory tasks without the full Active Directory platform, and it is independent of Active Directory Domain Services. Certificate Services is responsible for handling digital certificates and provides authentication and encryption as well. Federation Services specializes in SSO services (Single Sign-On) and facilitates the secure sharing of sensitive information. Rights

Management Services provides protection for sensitive information through identity, encryption, and authorization policies.

Active Directory Security Considerations

There are numerous security considerations to factor in when dealing with Active Directory. The two largest security risks faced by Active Directory are by far Insider threats and privilege escalation. Insider threats play a role in any organization's security posturing. Privilege escalation can come in the form of misconfiguration vulnerabilities or malicious activity by a bad actor. Misconfiguration can be a simple mistake, but that simple mistake may lead to a user having more access than intended. A bad actor also may seek unauthorized access to Active Directory and then use that access to further escalate their privileges. Fortunately, there are numerous ways to ensure the security of Active Directory.

Least privilege is a golden principle in Cybersecurity operations. The principle of least privilege entails the idea that a user should only be afforded the bare minimum permissions necessary to their job/role. Data encryption is another effective mitigation technique for Active Directory security concerns. Data encryption safeguards data and information in storage and in motion, thus adding an additional layer of security to the organization's posture. Employee cybersecurity awareness training is also crucial, as an organization's security framework is almost meaningless without properly trained and educated staff to help reinforce the framework.

There are further mitigation techniques available that may be optional, depending on the size and means of the organization. Intrusion detection and/or prevention infrastructure is incredibly beneficial as well. These systems function to alert administrators to nefarious activities and entry attempts on their networks. Having advanced notice, or even notice in real-time, can greatly increase the chances of successfully thwarting Active Directory threats.

Network segmentation is yet another powerful mitigation technique. Network segmentation entails dividing the network up into smaller individual components. With the network broken up into smaller segments – any potential incident or intrusion can be isolated to the affected network. With the incident or intrusion isolated, the remaining components of the network can continue their functions undisturbed while the affected network is attended to.

WORK CITED

Gladden, Malik. “Active Directory Components.” *Windows Systems for Cybersecurity*, 3 March 2026, Canvas, https://canvas.odu.edu/courses/202169/pages/04-%7C-active-directory-components?module_item_id=9604373

Gladden, Malik. “Managing Active Directory in Windows.” *Windows Systems for Cybersecurity*, 3 March 2026, Canvas, https://canvas.odu.edu/courses/202169/pages/04-%7C-managing-active-directory-in-windows?module_item_id=9604374

Gladden, Malik. “Mitigating Security Challenges.” *Windows Systems for Cybersecurity*, 3 March 2026, Canvas, https://canvas.odu.edu/courses/202169/pages/04-%7C-mitigating-security-challenges?module_item_id=9604375

“What Is Active Directory? (AD) - Definition, Benefits & More: Proofpoint Us.” *Proofpoint*, 10 June 2025, www.proofpoint.com/us/threat-reference/active-directory.

Harwood, Robin. “Best Practices for Securing Active Directory.” *Microsoft Learn*, learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory. Accessed 4 Mar. 2026.