

Gunay Maharramli
202302 Guided Research Grad I
George Washington University & ADA University
Data Privacy and Security in Database System
Report IV

This week, I focused on implementing LDAP (Lightweight Directory Access Protocol) authentication, a method to enhance the security of our system. Actually, PostgreSQL offers diverse external authentication options, encompassing GSSAPI, LDAP, and RADIUS. GSSAPI, also known as Generic Security Service Application Program Interface, employs Kerberos for user authentication. Meanwhile, LDAP, which stands for Lightweight Directory Access Protocol, verifies users by connecting to an LDAP server. Due to the following reasons, I choose LDAP as the preferred authentication method. Its balanced combination of performance and simplicity for installation and maintenance, along with its efficiency in network bandwidth usage and high-performance encrypted transmission, make it the ideal choice for our authentication needs. The process involved ensuring that only valid user name and password combinations are verified using LDAP, while other aspects of the authentication mechanism remained unaffected. Only the user name and password combinations are validated using LDAP. Therefore, before LDAP can be used for authentication, the user must already be present in the database. With the dedicated support and expertise of the system administrator, the LDAP configuration for the Active Directory was successfully completed.

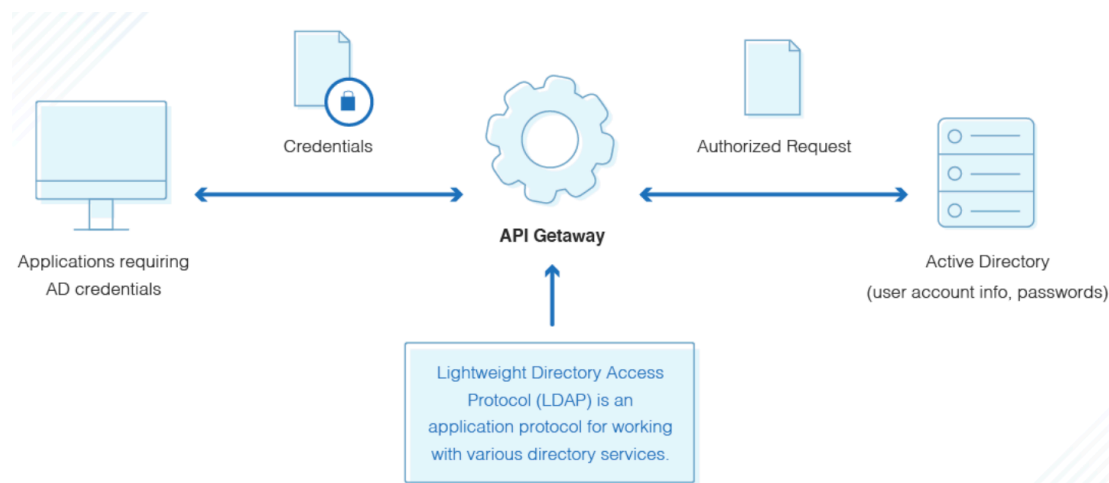


Figure 1. LDAP Authentication for Active Directory.

Active Directory plays a vital role in safeguarding the security of your IT systems, with LDAP serving as a fundamental component of its functionality. Consequently, both Active Directory and LDAP are indispensable for maintaining the overall security of your IT environment. Active Directory functions as a user management directory service. It helps control all network devices like computers, printers, and mobile devices, along with associated users. By assigning privileges, you can manage access to objects and information in Active Directory. Active Directory authentication is crucial as it controls access to important directory information, greatly impacting system security. The directory services act as a centralized repository, like a comprehensive phonebook, holding vital details about your organization, from devices to valuable information.

In the provided images, a clear distinction between LDAP authentication and non-LDAP configurations is evident. The primary dissimilarity lies in how LDAP authentication verifies the user's existence in the Active Directory, as specified in the PostgreSQL configuration file. When LDAP authentication is employed, it thoroughly examines whether the user is present in the specified level of the Active Directory. If the user is not found, or if the provided password and username do not match, an error is triggered, and access to the system is denied, ensuring a stringent security measure.

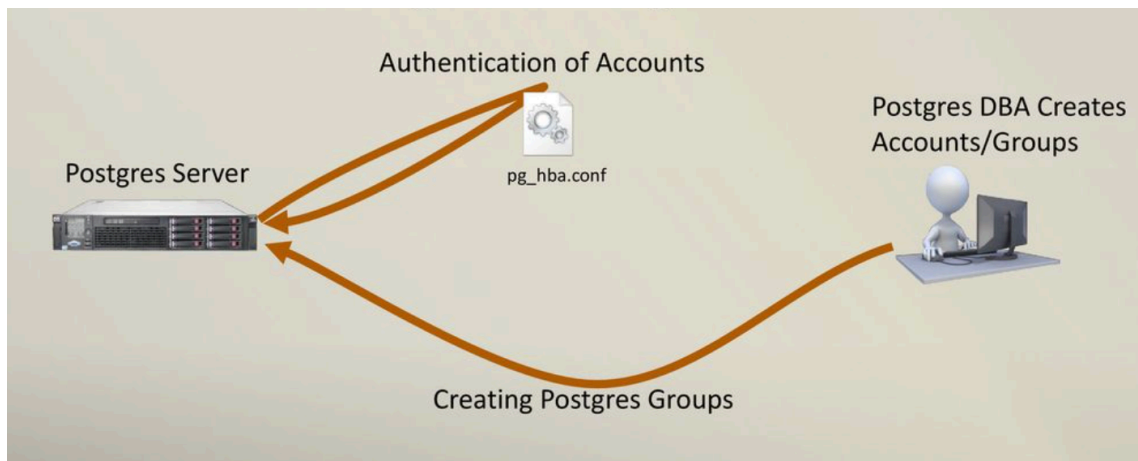


Figure 2. Non-LDAP Postgres Configuration.

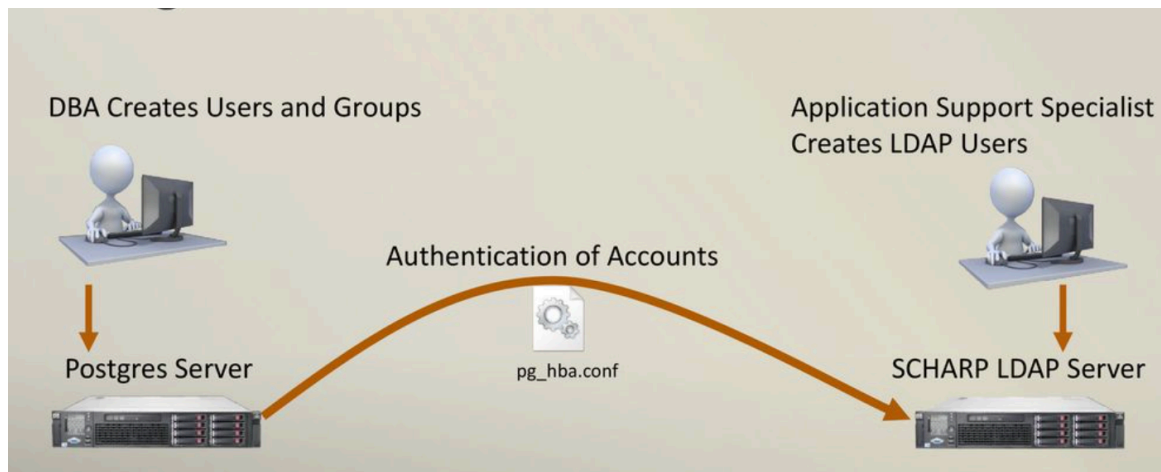


Figure 3. Postgres with LDAP Authentication.