Unified Authentication, Authorization and User Administration - An Open Source Approach

by Ted C. Cheng

Authentication, authorization, and user administration are critical components in secure enterprise computing. This talk presents a unified architecture for authentication, authorization, and user administration for Linux and Unix-variant environments. The architecture aims at providing robustness, performance, scalability, high availability, and low total cost of ownership (TCO) for enterprise deployments, while preserving the compatibility with existing IT infrastructure. The design scales vertically and horizontally by distributing workload among multiple OpenLDAP servers. The flexible cache configuration minimizes network access traffic, delivering the high performance demanded by enterprise business needs. The design offers high availability via the LDAP Sync Replication (syncrepl) services.

Enterprises can deploy services in a modular and scalable manner based on corporate geographical regions and organizational units. One or more servers can be deployed for each geographical region to minimize cross-region access latency. Clients can further be configured to access services for their respective organizational units from the regional servers. The cache configuration on the client systems stores information locally, eliminating redundant accesses to the regional but remote servers. This is particularly critical for heavily loaded systems in which repeated service requests for the same information can be handled via local cache.

The design of the unified authentication, authorization, and user administration architecture is the result of the cumulative efforts of the open source community in the past many years, involving technologies such as Name Service Switch (NSS), Network Information Services (NIS/NIS+), Domain Name Services (DNS), Pluggable Authentication Modules (PAM), Lightweight Directory Access Protocol (LDAP), LDAP Content Synchronization, Secure Socket Layer/Transport Layer Security (SSL/TLS), OpenLDAP SLAPD, and so on.

This presentation provides an overview of the architecture and focuses on two distinct enhancements, i.e., LDAP client-side caching and disconnected operations, using the OpenLDAP Name-Service Overlay (nssov) and the Proxy Cache engine. The nssov overlay improves the robustness of the design by addressing many issues in the PADL approach, while the Proxy Cache engine offers persistent caching capability and takes advantage of the connection pooling of the ldap backend.