

# LDAPCon 2015

## Title

Introducing a Security Access Control Engine that resides in OpenLDAP

## Type

45 Minute Technical Presentation

## Abstract

The OpenLDAP Accelerator is a security Policy Decision Point (PDP) that resides inside the slapd process to allow better functionality/performance than otherwise would be possible. This presentation introduces the new technology that is based on LDAPv3 extended operations, its rationale, and how it works. We'll explore the idea of protocol standardization to promote interoperability across directory implementations. At the end will be a live demo to illustrate the value proposition of this unique design.

## Outline

1. Introduction
2. Rationale
  - functionality
  - performance
  - practicality
3. System Architecture
4. Client-Side Components
  - Policy Enforcement Points (PEP):
  - Java
  - C
  - Python
  - ...
5. Server Side Component
  - PDP:

- OpenLDAP slapo-rbac Overlay

## 6. Functional Model

- IETF Draft Proposal
- LDAPv3 Extended Operations
- RBAC System Functions:
  - createSession
  - checkAccess
  - addActiveRole
  - dropActiveRole
  - userRoles
  - sessionPermissions

## 7. Logical Model

- IETF Draft Proposal (first discussed at ldapcon2013)
- RBAC Entities:
  - Users
  - Roles
  - Permissions
  - Sessions
  - Audit Log

## 8. Management of Data and Policies

- Apache Fortress Core

## 9. Performance

- < 1ms response time under load

## 10. Demo

- Micro-Benchmark
- Use Cases
- Audit Trail

## 11. Questions

### **Biography**

System Architect at Symas. Member of the OpenLDAP Engineering Team. Apache Directory PMC.