Open Source IAM using Fortress and OpenLDAP

LDAPCon
October 11, 2011

Shawn.McKinney@JoshuaTreeSoftware.us
Agenda

- Product vision
- Project status
- Functional gaps covered
- Features and technologies
- Installation and usage demo
- Where to get more information
- Roadmap
- Questions
Vision

• OpenLDAP matured
  – the ‘ilities’
  – flexible data storage
  – auditing with access log
  – password policies

• Specifications formalized
  – RBAC, SAML, etc...

• Gaps persisted
  – between those that employ secure technology and who don’t

• Needs remain for
  – all networked applications to utilize adequate safeguards
  – a common and robust API that works across all platforms
  – the ubiquitous IAM infrastructure that is easy to use, cost effective and long term viable

• Opportunity exists
  – to harvest a large and previously untapped market share
Project Status

• Start date
  – Jan 2009

• Sponsor
  – JoshuaTree Software

• Partner
  – Symas

• Release Schedule
  – Oct 2011 – 1.0 – Fortress Core & Realm Client SDKs
  – Oct 2012 – 2.0 – Commander Admin UI Server
  – Apr 2013 – 3.0 – En Masse Policy Server
This engine is powered by OpenLDAP

- Capable, robust server infrastructure for LDAP v3 network protocols
- Reliable, scalable, fault tolerant, highly available with 99.99% uptime
- Comprehensive authentication support
- Flexible application data storage and retrieval
- Reliable audit event storage and retrieval
- Server-side password policy support
- Portability across system platforms
But

Functional Gaps
OpenLDAP doesn’t provide

- RBAC API/object model
- Delegated administration model for enterprises
- Comprehensive authorization and audit support
- Security enforcement with Java EE containers
- Password policy client-side APIs
- Tools to install/configure IAM infrastructure and maintain user and policy data
ANSI/NIST RBAC Compliance

- **RBAC0**: users, roles, perms, sessions
- **RBAC1**: hierarchical roles
- **RBAC2**: static separation of duties
- **RBAC3**: dynamic separation of duties
User and Role Temporal Constraints

- begin/end date
- begin/end time
- day of week
- temporary lockout periods
- timeout
Administrative Role Based Access Control (ARBAC02)

- administrative user access control
- user OUs
- perm OUs
- administrative roles (hierarchical)
- administrative permissions
Rationale
RBAC /ARBAC

- enterprise admin model
- reduce costs
- centralized policy control
- regulatory compliance
- code reuse
- separation of duty control

Diagram:
- Role Hierarchy
- Application
- Objects (OBJ)
- Operators (OPERS)
- Users (USERS)
- Sessions (SESSIONS)
- Permissions
- Administrative Objects (ADMIN OBJ)
- Administrative Operators (ADMIN OPERS)
- User OUs
- Admin OUs
- Role Hierarchy
- Admin Role Hierarchy
Audit and Monitoring

• Audit storage and retrieval
  – Session Creation Events
  – Authorization Events
  – Administrative Events/History
  – API for Monitoring and Reporting
Functional Gaps
Password Policy Compliance in Apps

PW Status
User Id: jdoe
locked: false
reset: false
last failure time: 13:47, 07/2/2011
grace time: NA
history:
policy: Consumer

Fortress SDK

OpenLDAP
Password Policy Gaps
Supported
Partial
Not Supported

USERS

Consumer
maxAge: indefinite
inHistory: 0
checkQuality: true
minLength: 8
expireWarning: NA
graceLoginLimit: 0
lockout: true
lockoutDuration: forever
maxFailure: 5
failureCountInterval: 5 mins
mustChange: true
allowUserChange: true
safeModify: true
...

Employee
maxAge: 90 days
inHistory: 5
checkQuality: true
minLength: 8
expireWarning: 10 days
graceLoginLimit: 3
lockout: true
lockoutDuration: 30 mins
maxFailure: 5
failureCountInterval: 5 mins
mustChange: true
allowUserChange: true
safeModify: true
...

Admin
maxAge: indefinite
inHistory: 0
checkQuality: false
minLength: 12
expireWarning: NA
graceLoginLimit: 0
lockout: false
lockoutDuration: NA
maxFailure: 0
failureCountInterval: 0
mustChange: false
allowUserChange: false
safeModify: false
...
Product Features
Fortress 1.0 Packages

1. **Embeddable Core SDK**
   - APIs for Java applications

2. **Pluggable Realm**
   - SPIs for Java EE Containers

3. **Builder Tools**
   - Server Installations
   - Platform specific
   - OpenLDAP binaries
   - Fortress binaries
Fortress Core SDK
Nine Managers, 100+ APIs

1. **AccessMgr** – enforcement for RBAC in Java apps
2. **AdminMgr** – provision RBAC objects and policies
3. **ReviewMgr** – interrogation of RBAC objects and policies
4. **PswdPolicyMgr** – provision and interrogate OpenLDAP password policies
5. **DelegatedAccessMgr** – enforcement for ARBAC in Java apps
6. **DelegatedAdminMgr** – provision ARBAC objects, policies
7. **DelegatedReviewMgr** – interrogate ARBAC objects and policies
8. **AuditMgr** – monitor audit data
9. **ConfigMgr** – provision properties for application usage of Fortress
Fortress Realm SPI
Policy Enforcement for Java EE Containers

• **RealmMgr** – runtime security policy enforcement for applications running within JEE containers
  – Websphere, JBoss, Tomcat available today
  – Glassfish & Weblogic available future

• **Declarative Enforcement**
  – Coarse-grained policy enforcement
  – Sessions, simple authentications, role-based authorizations, session management
  – Safe, secure and bullet-proof

• **Monitoring**
  – Security audit trail stored in OpenLDAP
Fortress Realm SPI
Classloader Isolation Technique

• keep runtime libraries off the app server’s execution classpath
• simple, predictable and repeatable installation outcome
Fortress Builder Package
Install, Configure, Administer

• Install and configure OpenLDAP servers
• Tailor OpenLDAP servers for Fortress usage
• Property persistence for Fortress apps
• Build and run load scripts (drive admin APIs)
• CRUD console for administration and review APIs
• Full regression testing of installations (all APIs)
• Encryption and decryption of application properties
• Samples to learn the programming APIs
Technologies in Use

Lines Of Code

- OpenLDAP: 49%
- Apache Commons: 25%
- UnboundID SDK: 15%
- Fortress SDK: 8%
- JGraphT: 3%
Fortress Builder & Calendar Sample
Where to get more

1. Collaboration and Source ---> OpenLDAP.org
   – GIT source repo:  http://www.openldap.org/devel/gitweb.cgi
   – list server:     http://www.openldap.org/lists/mm/listinfo/openldap-fortress
   – issue tracking:  http://www.openldap.org/its/index.cgi

2. Silver Release and Doc -> JoshuaTreeSoftware.us
   – doc:  https://joshuatreesoftware.us/jtspages/docs.php
   – release: https://joshuatreesoftware.us/jtspages/download.php

Roadmap

• 2.0 Commander Web UI Server
  – currently in development
  – Fortress & OpenLDAP administration
  – Java EE platform uses Apache **Wicket** UI framework
  – October 2012

• 3.0 En Masse Policy Server
  – RESTful API wrapper for **Fortress APIs**
  – Java EE platform uses Apache **CXF** & **Camel** frameworks
  – April 2013

• 4.0 Perimeter Server
  – B2C SSO
    • SSO Reverse Proxy Server
    • SAML 2.0
  – B2B SSO
    • WS-Trust Security Token Server
  – October 2013
Questions
Thank You!

Shawn.McKinney@JoshuaTreeSoftware.us