RBAC Enable Your Java Web Apps Using Apache Directory and Fortress

Shawn McKinney – SYMAS Corporation

April 15, 2015
Introduction

• Systems Architect @ Symas

• Committer @ OpenLDAP & Apache Directory Projects
Agenda

I. Project Overview
II. Components
III. Standards
IV. Future
V. Demo
VI. Benchmarks
VII. Wrap-up
I. Project Overview
Project Description

• High Performance Identity and Access Management

• Permission-based Access Control Model (RBAC)

• Four Components:
  • Core
  • Realm
  • Web
  • Rest
Project Features

• Highly Performant

• ANSI INCITS 359

• Multitenant data and object model

• Audit Trail (OpenLDAP only)

• LDAPv3 Portable
Project History

- Core & Realm released in '11 to OpenLDAP Project
- Rest component in '12 to OpenLDAP
- Web component in '13 to OpenLDAP
- Moved all to Apache Directory project in '14
## Project History

22 Releases

<table>
<thead>
<tr>
<th>Group</th>
<th>Artifact</th>
<th>Version</th>
<th>Age</th>
<th>Popularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>us.joshuatreesoftware</td>
<td>fortress</td>
<td>1.0-RC30</td>
<td>1.1 yrs</td>
<td></td>
</tr>
<tr>
<td>us.joshuatreesoftware</td>
<td>fortress</td>
<td>1.0-RC24</td>
<td>1.3 yrs</td>
<td></td>
</tr>
<tr>
<td>us.joshuatreesoftware</td>
<td>fortress</td>
<td>1.0-RC33</td>
<td>1.4 yrs</td>
<td></td>
</tr>
<tr>
<td>us.joshuatreesoftware</td>
<td>fortress</td>
<td>1.0-RC32</td>
<td>1.4 yrs</td>
<td></td>
</tr>
<tr>
<td>us.joshuatreesoftware</td>
<td>fortress</td>
<td>1.0-RC31</td>
<td>1.5 yrs</td>
<td></td>
</tr>
<tr>
<td>us.joshuatreesoftware</td>
<td>fortress</td>
<td>1.0-RC30</td>
<td>1.5 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC29</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC28</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC27</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC26</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC25</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC24</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC23</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC22</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC21</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC20</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC19</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC18</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC17</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC16</td>
<td>1.6 yrs</td>
<td></td>
</tr>
<tr>
<td>org.openldap</td>
<td>fortress</td>
<td>1.0-RC15</td>
<td>1.6 yrs</td>
<td></td>
</tr>
</tbody>
</table>

http://mvnrepository.com/artifact/us.joshuatreesoftware
http://mvnrepository.com/artifact/org.openldap
II. Components
Inventory of Components

- Accelerator – LDAPv3 Extended
- Core – APIs
- Realm – Policy Enforcement
- Web – HTML Server
- Rest – XML Server

108 k SLOC
Fortress Core

- Identity and Access Management SDK
- Communicates LDAPv3 protocol but has switch for REST
- Extensive Tests (one-to-one)

https://git-wip-us.apache.org/repos/asf/directory-fortress-core.git
Fortress Core Depends On

- Mostly other Apache components like
  - Commons
  - CXF
  - Directory
- With some help from
  - Javax
  - Jgrapht
  - ehcache
Core System Architecture

Legend
- Fortress
- LDAP
- HTTP
- Applications

FTP
HTTP/S
LDAP
HTTP
Applications

Legend
- J
- Java
- VM

OpenLDAP
LDAP/S
Native

OR

Apache DS
LDAP/S
Java VM

LDAP/S
Fortress Core
Java VM

Java App #2
HTTP/S

All APIs work with standard LDAPv3 protocols
Fortress Realm

- Policy enforcement and audit for java EE containers
- Simple deployment
- Uses context.xml for Tomcat integration
- Shares security session with the app

https://git-wip-us.apache.org/repos/asf/directory-fortress-realm.git
Fortress Rest

- HTTP Rest Server
- Uses Apache CXF
- Uses Fortress Core APIs and Domain model
- Secured with Fortress Realm

https://git-wip-us.apache.org/repos/asf/directory-fortress-enmasse.git
Integrate with 3rd party rest lib or Fortress Core to connect with Fortress Rest.
Fortress Web

- Administrative UI
- Uses Apache Wicket Framework
- Uses Fortress Core apis
- Secured with Fortress Realm

https://git-wip-us.apache.org/repos/asf/directory-fortress-commander.git
Option to use either HTTP or LDAPv3 protocol

Legend

- Fortress
- LDAP
- HTTP

Administrator

Web System Architecture
Fortress Accelerator

• Implements RBAC System Manager Functional Specs
• Policy Decision Point inside OpenLDAP
• Session state and audit trail inside OpenLDAP (LMDB)
• Communicates with LDAPv3 extended protocols
• Built for performance
Accelerator System Architecture

Legend

Fortress
LDAP
HTTP
Applications

OpenLDAP

RBAC Accelerator

LDAP/S Extended

Native

LDAP/S Extended

Other App

HTTP/S

Any Platform

Accel Client

Fortress Core

Java App #2

HTTP/S

Java VM

RBAC policy decision point (PDP)

RBAC policy enforcement may use extended ldap protocols to enhance performance
III. Standards
Inventory of Standards

- Role-Based Access Control (ANSI RBAC INCITS 359)
- Administrative Role-Based Access Control (ARBAC02)
- IETF Password Policies
- Java EE Security
- LDAPv3
More on RBAC

- RBAC0
  Users, Roles, Perms, Sessions
- RBAC1
  Hierarchial Roles
- RBAC2
  Static Separation of Duties (SSD)
- RBAC3
  Dynamic Separation of Duties (DSD)

http://csrc.nist.gov/groups/SNS/rbac/
More on ARBAC02

- Delegated Administration
- Object Model: AdminRoles, AdminPerms, User Orgs, Perm Orgs
- Functional Model: Delegated Admin Mgr, Delegated Review Mgr, Delegated Access Mgr

http://profsandhu.com/journals/tissec/p113-oh.pdf
IV. Future
Future Roadmap

• IETF RBAC Standardization
• Accelerator and Audit for Apache Directory Server
• Web Access Management / SSO
• Make the REST services **really** restful
• Policy Enforcement Modules for:
  • common linux distros
  • common web framework
  • other languages like C, Python, Ruby, …
More on IETF Standardization

- Encourage interoperability across directories
- Standard RBAC Object Model (LDAP Schema)
- Standard RBAC Functional Model (LDAPv3 operations)
Future Think

- ANSI RBAC Policy Enhanced
- Attribute-Based Access Control
- XACML
- OAuth 2 & UMA
V. Demo
Demo – Web Integration

- Wicket Sample Project on Github

https://github.com/shawnmckinney/wicket-sample
Demo Takeaways

• Need policy enforcement points (PEP) for...
  • Web frameworks (wicket, spring, ...)
  • Servlet containers (tomcat, jboss, ...)
  • Operating systems (fedora, debian, ...)
  • Cloud based systems (openstack, foundry, ...)
VI. Benchmark
Benchmark Overview

Measure the time to perform checkAccess method.

1. OpenLDAP Accelerator, Audit On
2. OpenLDAP, Audit On
3. OpenLDAP, Audit Off
4. ApacheDS, Audit Off
Benchmark Client

Machine Details:
• Ubuntu 13.04, 3.8.0-32-generic
• Intel® Core™ i7-4702MQ CPU @ 2.20GHz × 8
• 16GB

One Machine Process:
• Java version 7
• Running mvn -Ploadtest-fortress jmeter:jmeter
• 25 threads X 50,000 iterations of checkAccess
• 1,250,000 total invocations
Benchmark Server

Machine Details:
• Ubuntu 14.04
• 3.13.0-32-generic
• Intel® Core™ i7-4980HQ CPU @ 2.80GHz × 4
• 8GB
• SSD

Two Machine Processes:
• OpenLDAP 2.4.39 (w/LMDB)
• ApacheDS 2.0.0-M19 (w/ Mavibot)
Benchmark Results

1. OpenLDAP w/ Accelerator, Audit On
   • 11,533 TPS, 1 ms avg response
2. OpenLDAP, Audit On
   • 7,501 TPS, 2 ms avg response
3. OpenLDAP, Audit Off
   • 16,847 TPS, 0 ms avg response *
4. ApacheDS, Audit Off
   • 9,555 TPS, 2 ms avg response

* response time < 1 ms can't be measured with current test methods
VII. Wrap-up
1. Apache Fortress Project
   - http://directory.apache.org/fortress/
2. Apache Fortress End-to-End Security Tutorial
   - https://github.com/shawnmckinney/apache-fortress-demo
   - John Field
4. IAM Fortress Blog
   - https://iamfortress.wordpress.com/
More on Apache Fortress Demo

Requirements Covered

1. Java EE Authentication
2. Confidentiality
3. Coarse-grained AuthZ
   - Java EE
   - Spring
4. Fine-grained AuthZ

https://github.com/shawnmckinney/apache-fortress-demo