


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

APACHE CON
NORTH AMERICA

- 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

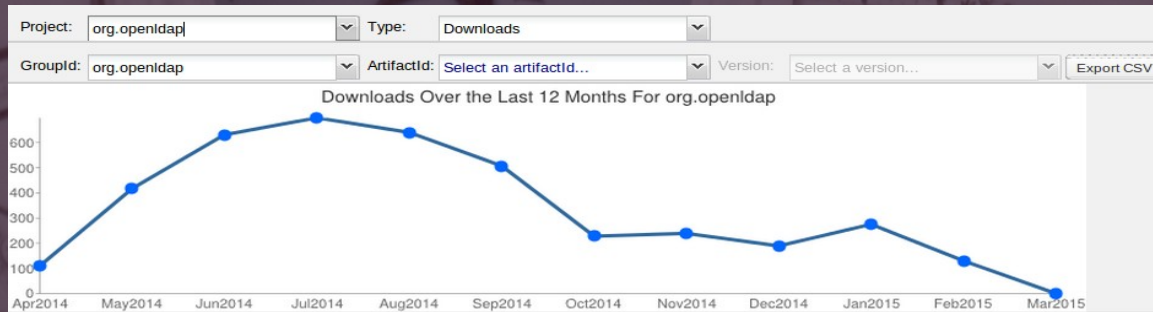
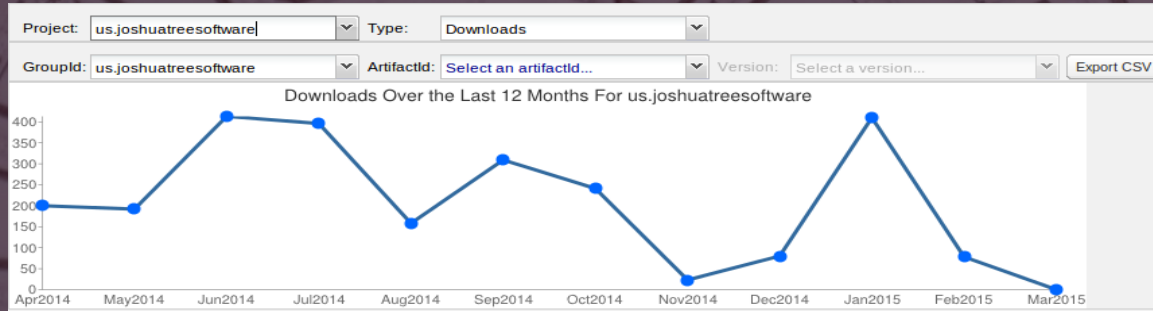
22 Releases

Group	Artifact	Version	Age	Popularity
us.joshuatreesoftware	fortress	1.0-RC35	1.1 yrs	
us.joshuatreesoftware	fortress	1.0-RC34	1.3 yrs	
us.joshuatreesoftware	fortress	1.0-RC33	1.4 yrs	
us.joshuatreesoftware	fortress	1.0-RC32	1.4 yrs	
us.joshuatreesoftware	fortress	1.0-RC31	1.5 yrs	
us.joshuatreesoftware	fortress	1.0-RC30	1.5 yrs	
us.joshuatreesoftware	fortress	1.0-RC29	1.6 yrs	
us.joshuatreesoftware	fortress	1.0-RC28	1.6 yrs	
us.joshuatreesoftware	fortress	1.0-RC27	1.8 yrs	
us.joshuatreesoftware	fortress	1.0-RC26	1.8 yrs	
us.joshuatreesoftware	fortress	1.0-RC25	1.9 yrs	
us.joshuatreesoftware	fortress	1.0-RC24	2.0 yrs	
us.joshuatreesoftware	fortress	1.0-RC23	2.1 yrs	
us.joshuatreesoftware	fortress	1.0-RC22	2.2 yrs	
us.joshuatreesoftware	fortress	1.0-RC21	2.2 yrs	
us.joshuatreesoftware	fortress	1.0-RC20	2.3 yrs	
us.joshuatreesoftware	fortress	1.0-RC19	2.3 yrs	
us.joshuatreesoftware	fortress	1.0-RC18	2.3 yrs	
org.openldap	fortress	1.0-RC39	236 d	
org.openldap	fortress	1.0-RC38	271 d	
org.openldap	fortress	1.0-RC37	309 d	
org.openldap	fortress	1.0-RC36	340 d	

<http://mvnrepository.com/artifact/us.joshuatreesoftware>
<http://mvnrepository.com/artifact/org.openldap>

Project History

Downloads

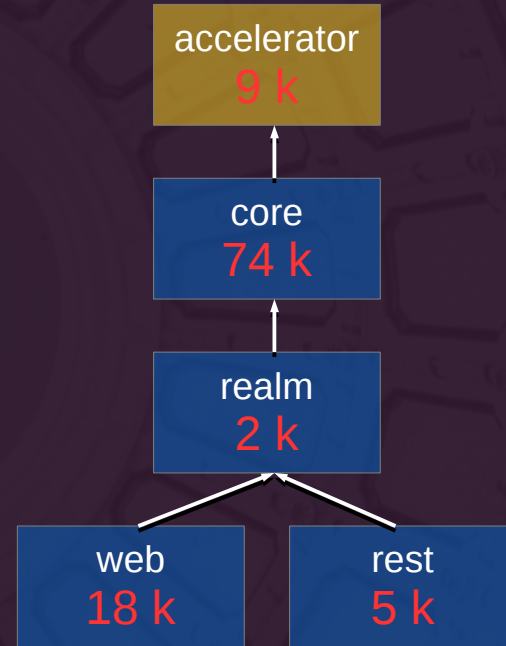




II. Components

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)

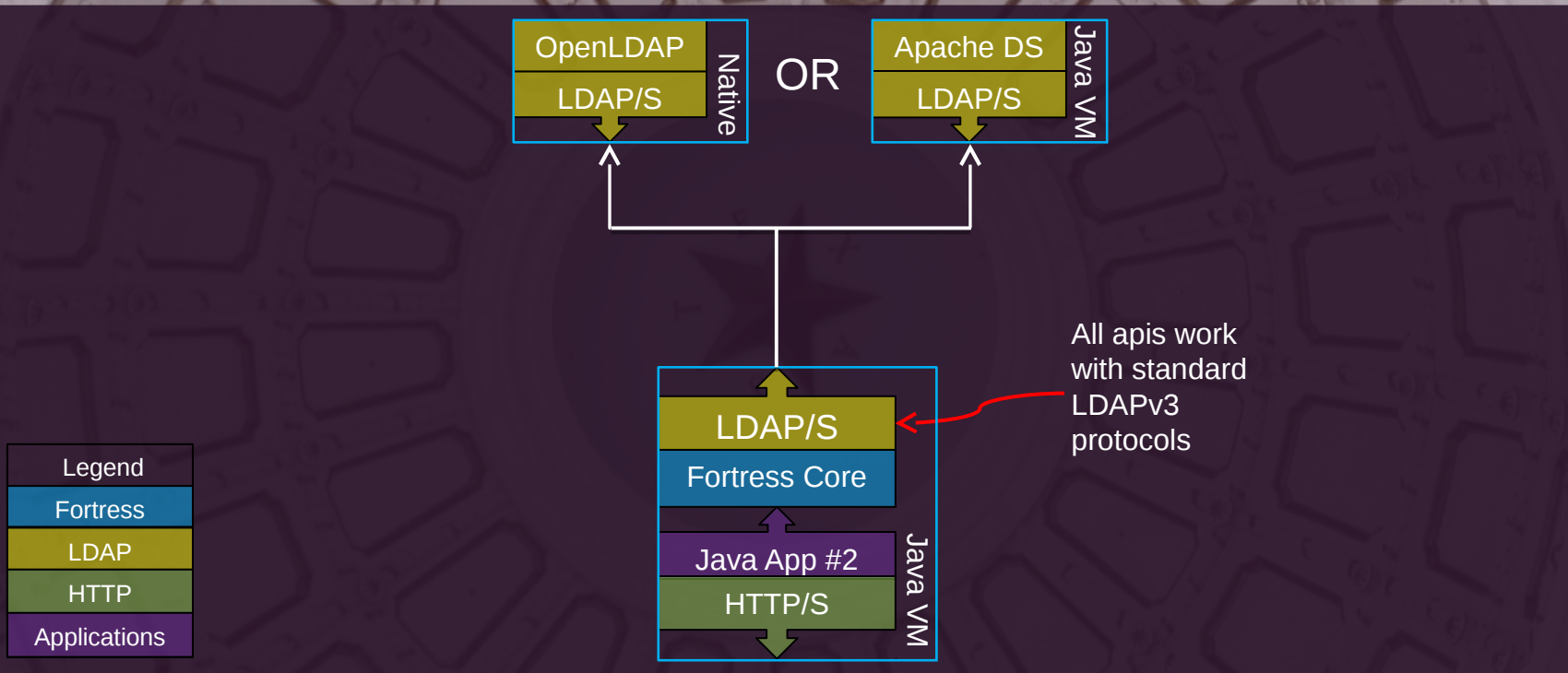


Fortress Core Depends On

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



Core System Architecture



Fortress Realm

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



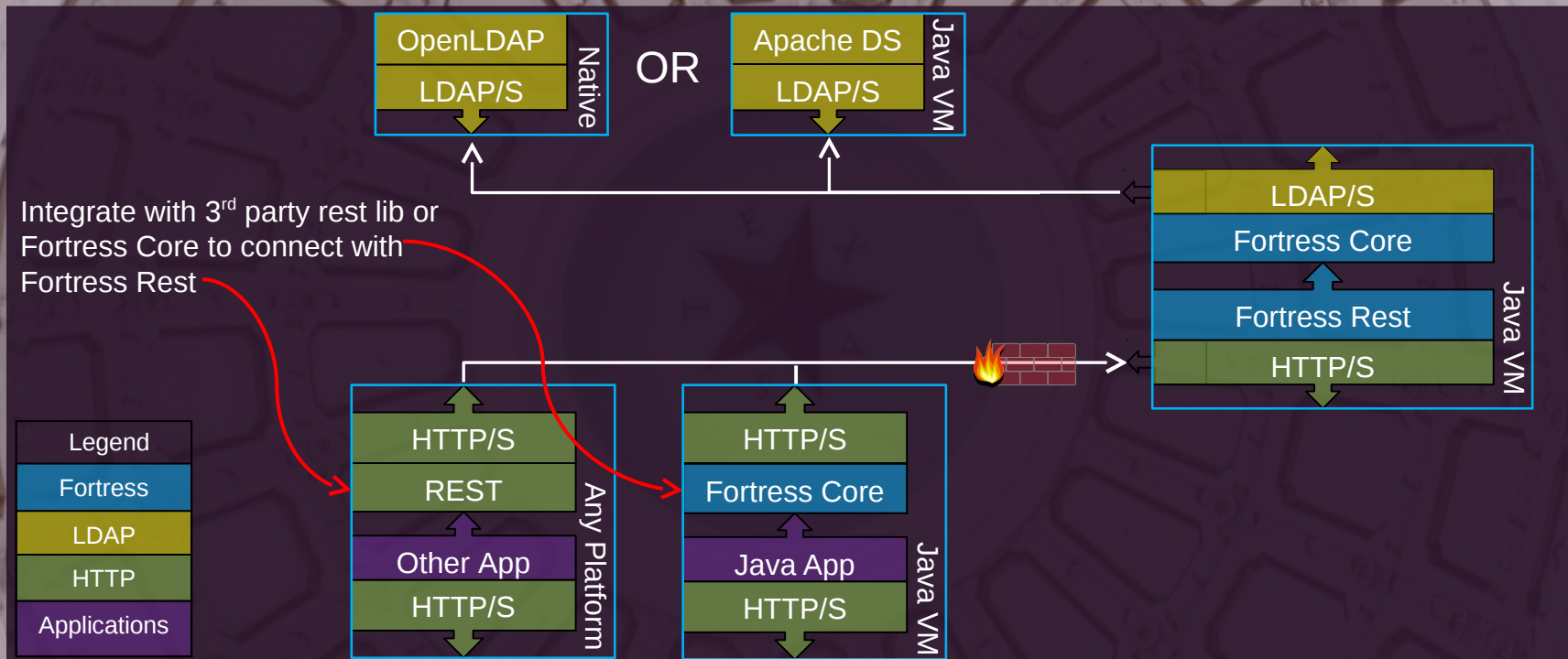
Fortress Rest

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



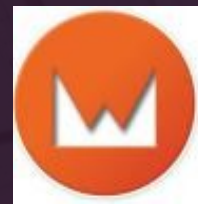
<https://git-wip-us.apache.org/repos/asf/directory-fortress-enmasse.git>

Rest System Architecture



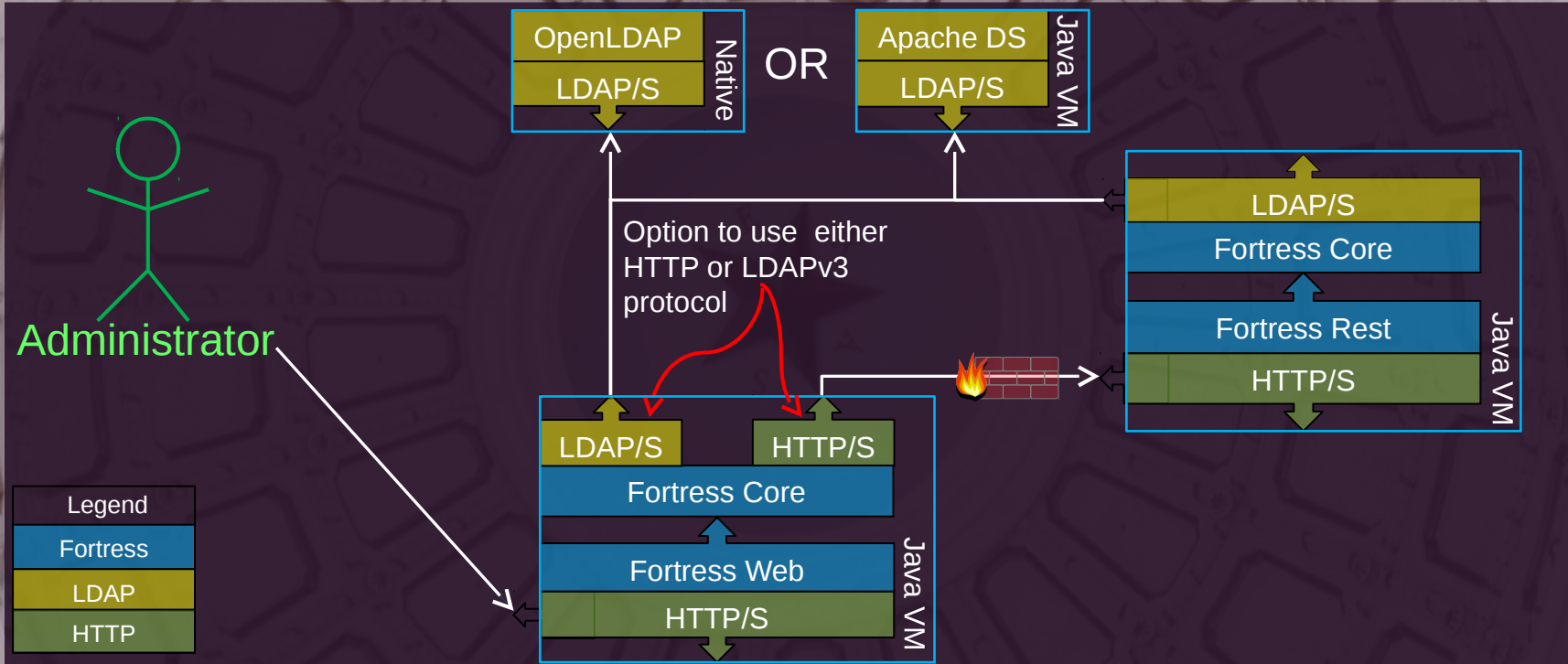
Fortress Web

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



The screenshot displays the Fortress Web RBAC Administration interface. At the top, there are navigation tabs for 'Program Links' including 'USERS', 'ROLES', 'PERMS', 'SSOS', 'SSDS', 'USERS', 'DUPMS', 'ADMLES', 'ADMOSIS', 'ADMPPMS', and 'LOGOUT'. Below this is the 'User Administration' section, which includes a search bar and a table of users. The table has columns for 'Users', 'User Organization', 'Description', 'Address', 'City', 'State', and 'RBAC Role Assignments'. The 'Users' column lists various user IDs, and the 'RBAC Role Assignments' column lists role names like 'jstjtu1user9'. To the right of the table, there is a detailed view for a selected user, showing 'RBAC Role Assignments', a calendar for 'Begin Time', and 'Contact Information for: LawrenceKS6604'.

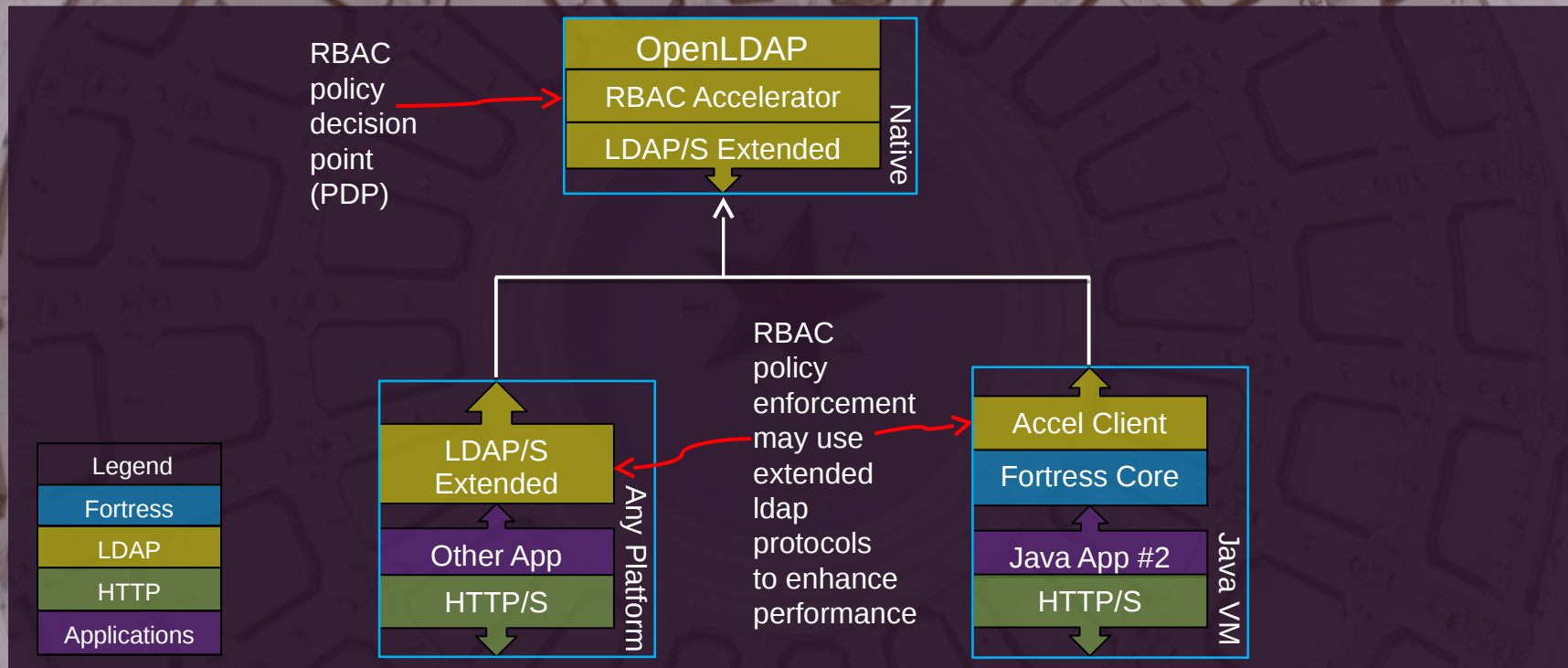
Web System Architecture



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





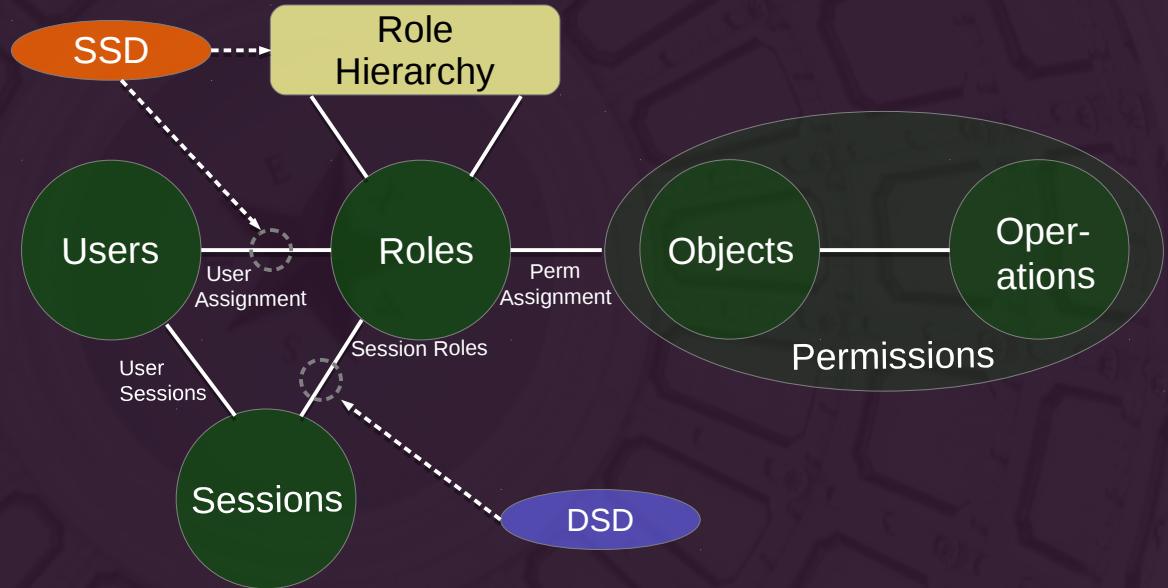
III. Standards

Inventory of Standards

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

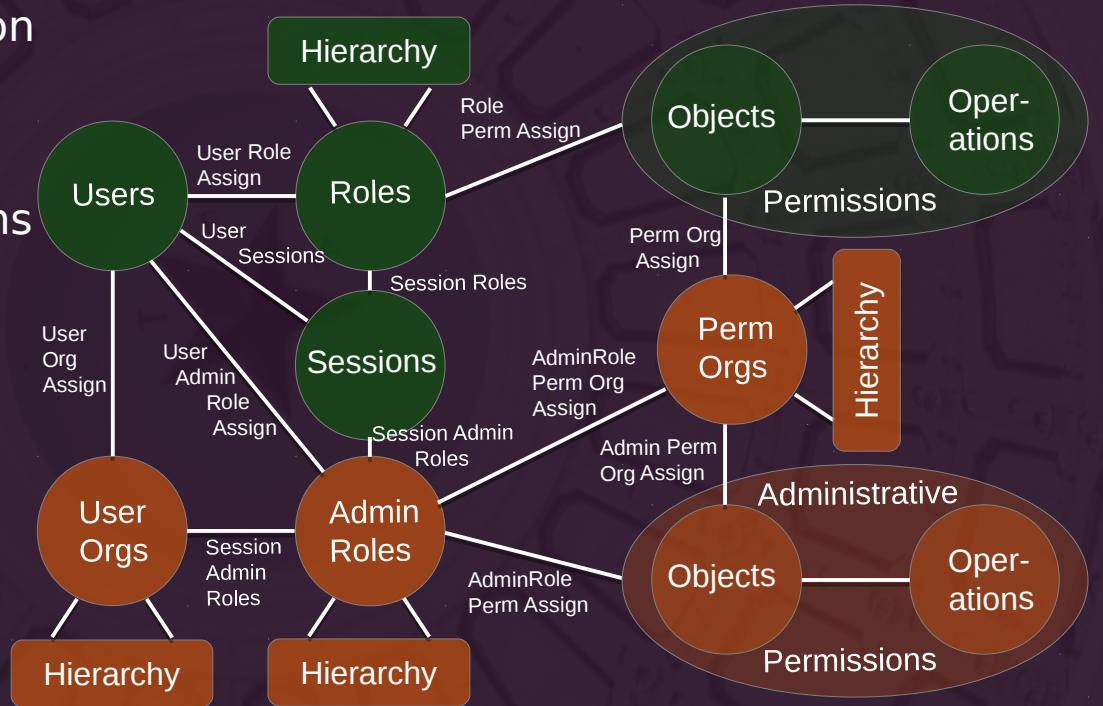
More on RBAC

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



More on ARBAC02

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



Legend

RBAC

ARBAC

<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)

- ANSI RBAC Policy Enhanced
- Attribute-Based Access Control
- XACML
- OAuth 2 & UMA



V. Demo

Demo - Web Integration

- Wicket Sample Project on Github

Wicket Sample Project

localhost:8080/wicket-sample/wicket/bookmarkable/org.wicket.sample.Page1?0

[PAGE1](#) [PAGE2](#) [PAGE3](#) [LOGOUT](#)

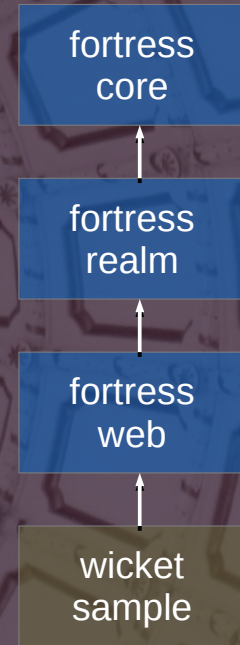
Page1

This is Page1

These buttons are secured by the following RBAC permissions

page1.button1	Object: Page1; Operation: Button1;
page1.button2	Object: Page1; Operation: Button2;
page1.button3	Object: Page1; Operation: Button3;

[WICKET AJAX DEBUG](#)



<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>

3. The Anatomy of a Secure Web App Using Java EE, Spring and Apache Directory Fortress

- John Field

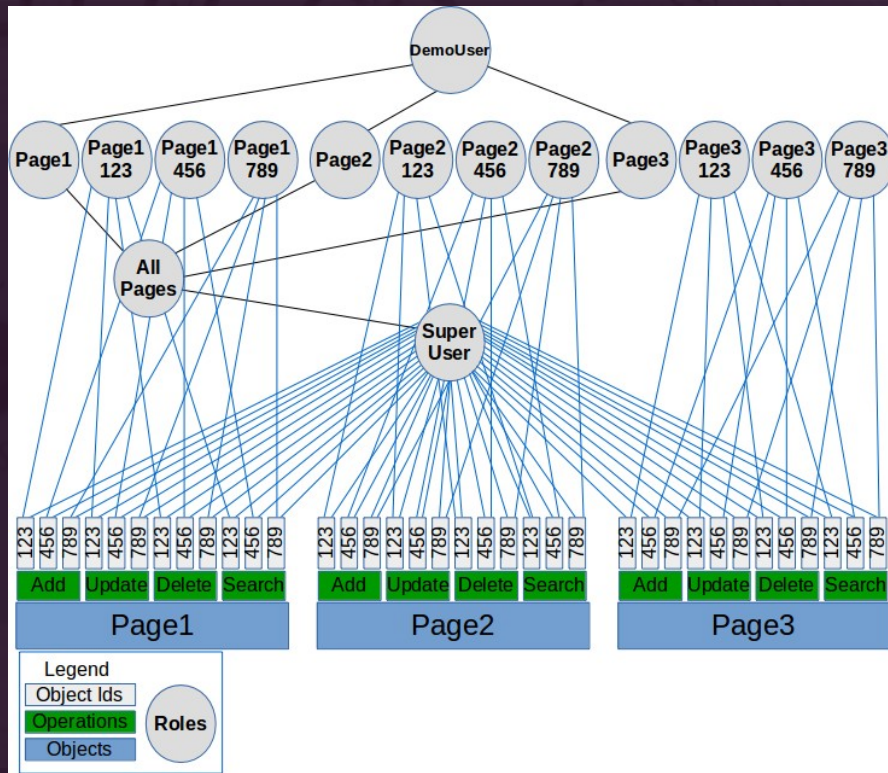
4. IAM Fortress Blog

- <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





[@shawnmckinney](#)
smckinney@apache.org

APACHE CON
NORTH AMERICA