BOF2337

Open Source Identity and Access Management Expert Panel, Part II

23 September 2013 5:30p

Hilton - Golden Gate 6/7/8

San Francisco CA

Expert Panel

- Emmanuel Lécharny, Apache Software Foundation
- Howard Chu, Symas
- Matthew Hardin, Symas
- Mike Schwartz, Gluu
- Shawn McKinney, JoshuaTree Software

23 September 2013 *San Francisco CA*

Agenda

- Open Source Access Control Stack
  - Overview
  - Introduce Enforcement Foundry

1. Base
   - Howard - OpenLDAP
   - Emmanuel - ApacheDS
2. Core
   - Shawn – Fortress
3. Perimeter
   - Michael – OX
   - Matt – Sentry
4. Discussion/Questions

Open Source Access Control Stack

- Standards-based IAM
- Several products fit this category
- End-to-end control of security functionality
- Connect apps and systems into a *centralized* and *multitenant* directory for authentication, authorization, provisioning and audit.
- Saves via lowered license, hardware, labor, power and space utilization

Three Component Types

1. Perimeter
2. Core
3. Base

Perimeter Provides

- Policy Enforcement Point (PEP) servers and APIs
  - Authorization, SSO & Federation
- Policy enforcement for…
  - web, java, system and native platforms
  - mobile, win, mac, unix, linux and mainframe
- Standards-based Access Control
  - SAML, UMA, OpenID Connect & RBAC
- Standards-based Provisioning
  - System for Cross-domain Identity Management (SCIM)

Core Provides

- Policy Decision Point (PDP) servers & APIs
  - APIs and services to communicate access decisions
  - One or more of these standards-based algorithms may be used:
    - RBAC, Rule, ABAC, XACML
- Policy Administration Point (PAP) Servers
  - Administration of access management policies including Users, Passwords, Roles, Permissions, etc…
  - APIs, Services and GUI's
  - Privileged Identity Management
  - LDAPv3 protocols with Base components
  - HTTP protocols with Perimeter components
- LDAP configuration and management tools

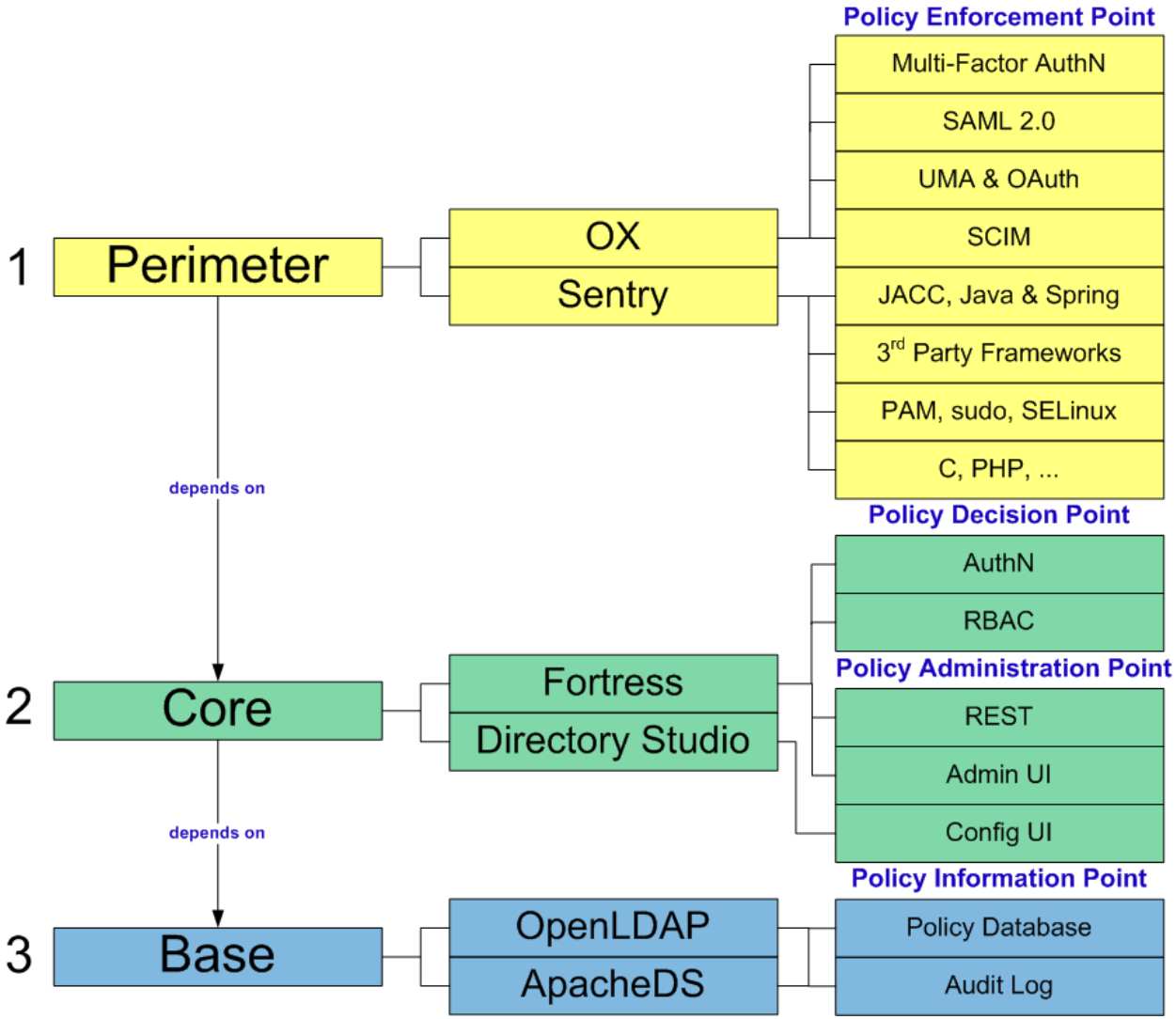
Base Provides

- Directory and Database Servers & APIs
- Extension mechanisms to support ever changing requirements
- Where the ‘ilities’ reside
  - Reliability
  - Scalability
  - Availability
  - Maintainability
  - Extendability
  - Compatibility

Introduce Enforcement Foundry

1. Perimeter
   - OX & Sentry
2. Core
   - Fortress
3. Base
   - OpenLDAP & Apache Directory Server

The Enforcement Foundry Stack



Communities

- ApacheDS
  - http://directory.apache.org/
- Enforcement Foundry
  - http://symas.com/products/symas-enforcement-foundry/
- Fortress
  - http://iamfortress.org/
- Gluu
  - http://www.gluu.org/
- OpenLDAP
  - http://www.openldap.org/

Howard Chu

- CTO, Symas
- Specialist in distributed information technologies including X.500/LDAP at University of Michigan. Experience at JPL, Locus Computing, and PLATINUM technology. Member and Chief Architect of the OpenLDAP Core Team.

Base Server - 

symas

- Written in C
  - but still multi-platform
- Reference implementation for LDAPv3
  - De-facto standard for LDAPv3
- Flexible access management extensions
  - SASL, Password policy overlay, Auditing overlay,
  - RBAC overlay (under construction)
  - BackSQL, Translucency
- Fastest LDAP server
  - Lightning Memory-Mapped Database (LMDB)
- Most dependable LDAP server
  - 99.99% uptime

JavaOne

Emmanuel Lécharny

- Core developer and member of the Apache Software Foundation™. Active contributor to the Apache Directory Server™ project, current chairman of the Apache MINA™ project. Previous positions include Technical Officer at Atos and Technical Committee Member for Wanadoo, the Orange ISP.

Base Server - ApacheDS

IKTEK
La Gestion d'Identité Open Source

- Written in Java
  - runs on all platforms
- LDAPv3 compliant
  - works with any LDAPv3 client
- Mature and ready for production
- Easy to use, maintain and test
  - ideal for developers to run on their local machines
- Performant
  - new backend
- Runs embedded or as standalone process
- Can be used as caching server
  - server runs with our without network layer
  - replicas can run anywhere on the network

Shawn McKinney

- Principal, JoshuaTree Software
- Fortress developer on the OpenLDAP engineering team. Previously held positions at FIS as lead security architect and development manager responsible for delivery of Open Source identity solutions.

- shawn.mckinney@jts.us

Core - Fortress

- Written in Java
- Policy Decision Point
  - ANSI INCITS 359-2004 compliant
    - Java APIs (Fortress Core)
    - REST services (En Masse)
- Policy Administration Point
  - ANSI INCITS 359-2004 compliant
    - Java APIs (Fortress Core)
    - REST services (En Masse)
    - Web GUI (Commander)
      - Delegated Administration
- Audit Trail
  - Authentication – tracks who is accessing the system
  - Authorization – tracks who did what, when and where
  - Administration – tracks the changes made to the data

Mike Schwartz

- Mike has been an entrepreneur and identity specialist for over 18 years. He is the technical and business visionary behind Gluu, whose open source OX projects enables domains to centralize authentication and authorization using open standards like SAML and OAuth2.
- Founded Gluu in 2009

Perimeter - OX

- Written in Java
- Policy enforcement for Web-based systems
- SSO/Federation
  - SAML 2.0, OpenID Connect
- Authentication
  - Strong, Multi-factor, Workflows
- Authorization
  - OAuth, UMA
- Provisioning
  - SCIM

Matthew Hardin

- VP Engineering, Symas
- Core developer and development executive for user management, networking and file management products at Locus Computing and PLATINUM technology.

Perimeter - Sentry

- Written in Java, C and PHP
- ANSI RBAC policy enforcement for distributed systems:

1. Java application servers
   - Java EE Container managed security for
     - Tomcat, JBoss & Websphere
   - ** Java Authorization Contract for Containers
   - ** Java SE Security Manager
   - Spring Security Filters
   - Apache Wicket framework components
   - RBAC APIs
     - Access Control
     - Java APIs use either LDAPv3 or HTTP protocol to perform access control
2. Unix/Linux
   - Centralized User Management
     - PAM, * sudo, * SELinux
3. Other platforms
   - ** C, * PHP

- * roadmap
- ** under construction

Panel Questions

- Why would I want to use open source for IAM?
  - Isn't it bad for security?
  - How does that business model work?
  - What are the license types in play?
  - Do you have a dual license scheme?
- What are additional requirements for access management?
- Is this ready to use today?
- What about legacy apps?
- What new standards are gaining traction?
- What is missing here?
  - Identity synchronization
  - Enterprise SSO