safehaus

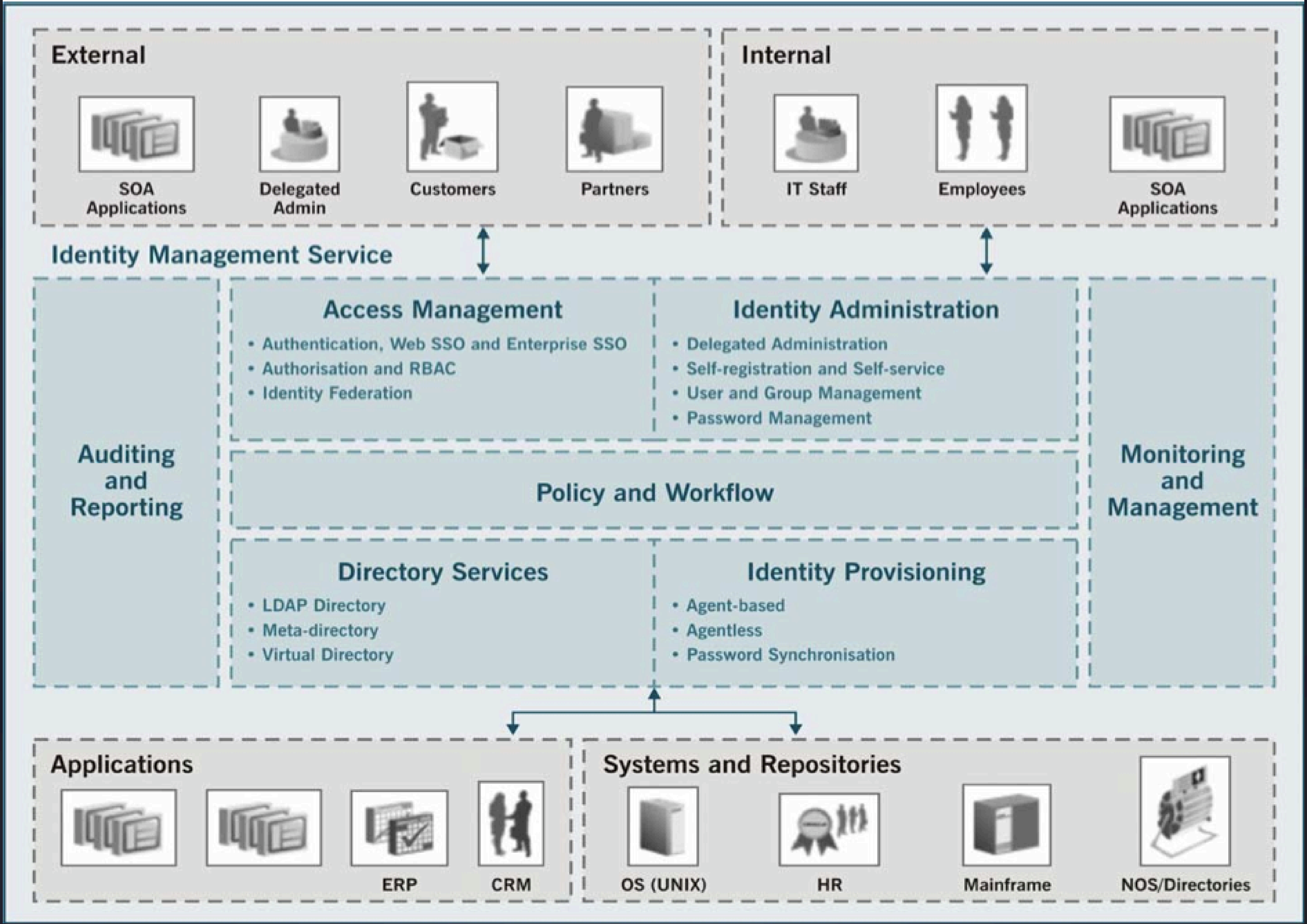
OSS Identity Management

How to leverage Open Source to manage your identity

jimyang@safehaus.org

Who am I

- Jim Yang
- 5 Years Identity Management Consultant
- Co-founder of Safehaus.org
- Project Lead of Penrose



External

SOA Applications

Delegated Admin

Customers

Partners

Internal

IT Staff

Employees

SOA Applications

Identity Management Service

Auditing and Reporting

Access Management

- Authentication, Web SSO and Enterprise SSO
- Authorisation and RBAC
- Identity Federation

Identity Administration

- Delegated Administration
- Self-registration and Self-service
- User and Group Management
- Password Management

Policy and Workflow

Directory Services

- LDAP Directory
- Meta-directory
- Virtual Directory

Identity Provisioning

- Agent-based
- Agentless
- Password Synchronisation

Monitoring and Management

Applications

ERP

CRM

Systems and Repositories

OS (UNIX)

HR

Mainframe

NOS/Directories

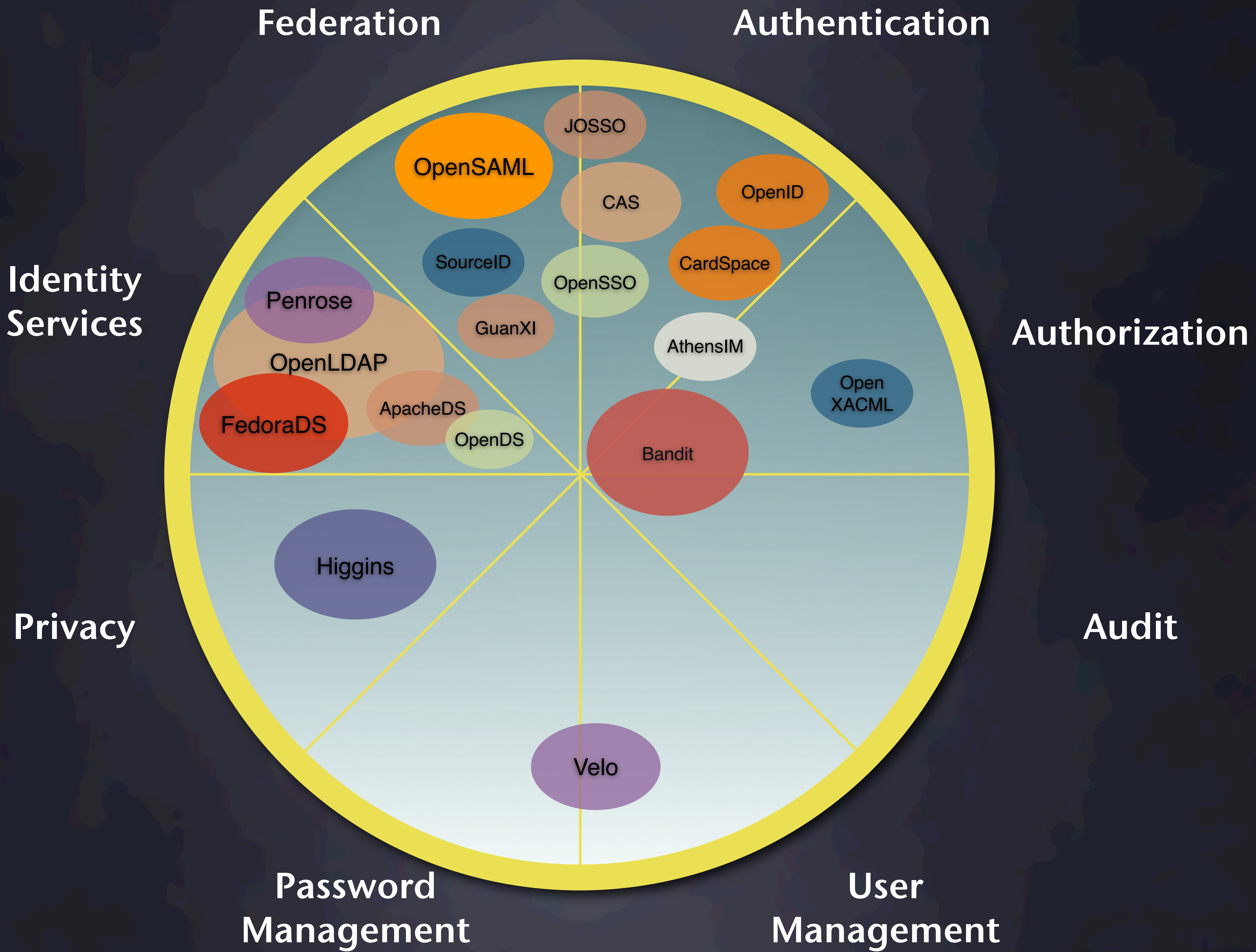
Identity Management Vendor (1)

	CA	Microsoft	IBM	Oracle	Sun
Infrastructure	eTrust DS	Active Directory	Tivoli DS	OID	JS DSEE OpenDS *
Identity Integration		MIIS	Meta Merge	OVD	
Access Management	Site/Id Minder		Tivoli FIM (TAMeb)	OAM OIM	JS AM OpenSSO *
Provisioning	ET Admin / eProv	MIIS	Access360	Thor	JS IM
Compliance	EEM				
Federation	Ping (OEM)	ADFS	Tivoli FIM		
Suite	CA IAM	ILM	Tivoli	Oracle AM	Sun JES

Identity Management Vendor (2)

	HP	BMC	Novell	Entrust	Evidian
Infrastructure	Netscape/ Redhat DS		eDirectory	Authority	
Identity Integration	Select Identity	Calendra			
Access Management	Select Access	Open Network	Novell IM,AM		SAM Web / SAM J2EE
Provisioning					
Compliance	Select Audit				
Federation	Select Federation				
Suite	OpenView Select Access	Control-SA IDM	NSure	GetAccess	

Open Source IdM Projects


Federation

Authentication

Identity Services

Authorization

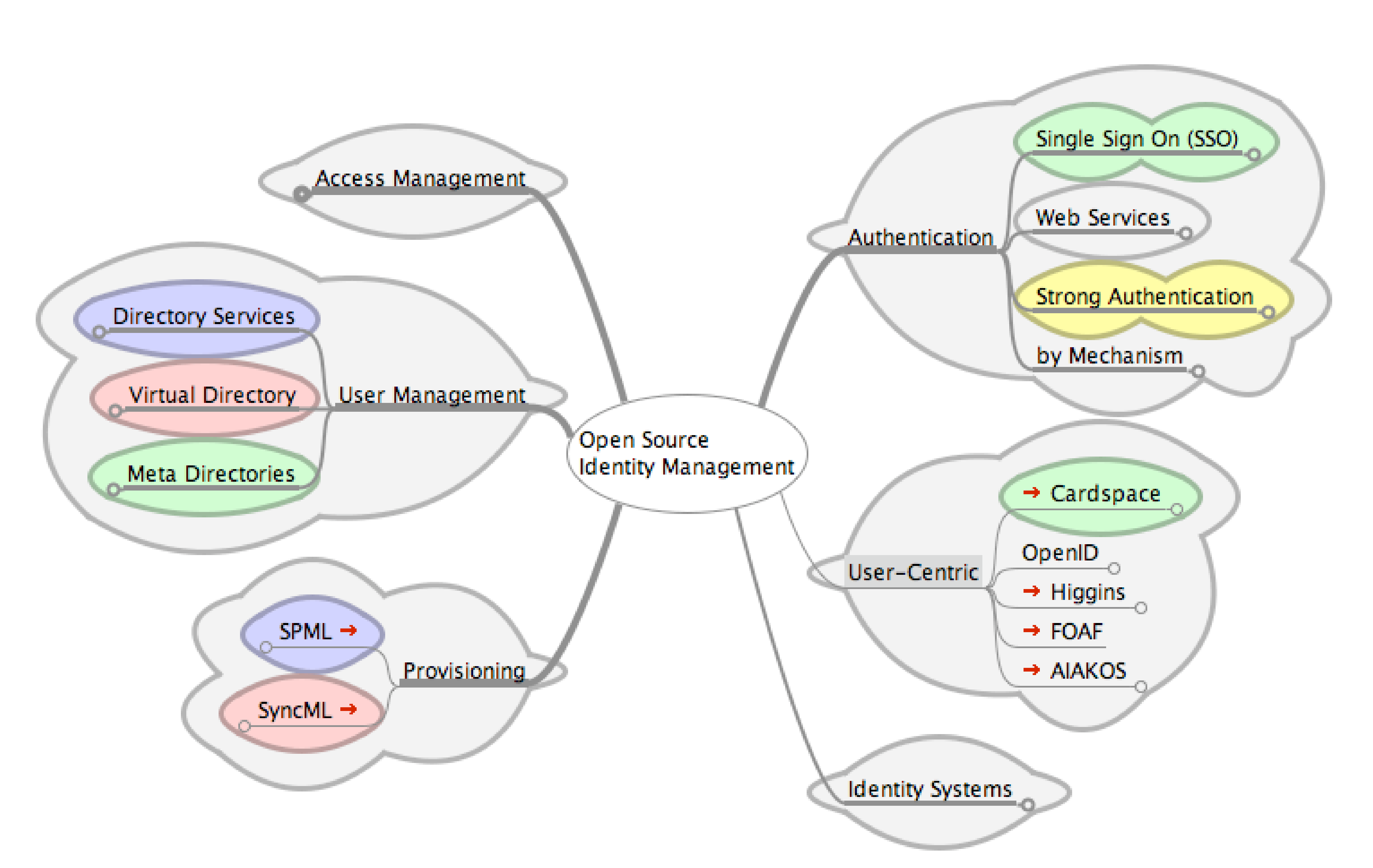
Privacy

Audit

Password Management

User Management

OSS Identity Management Map



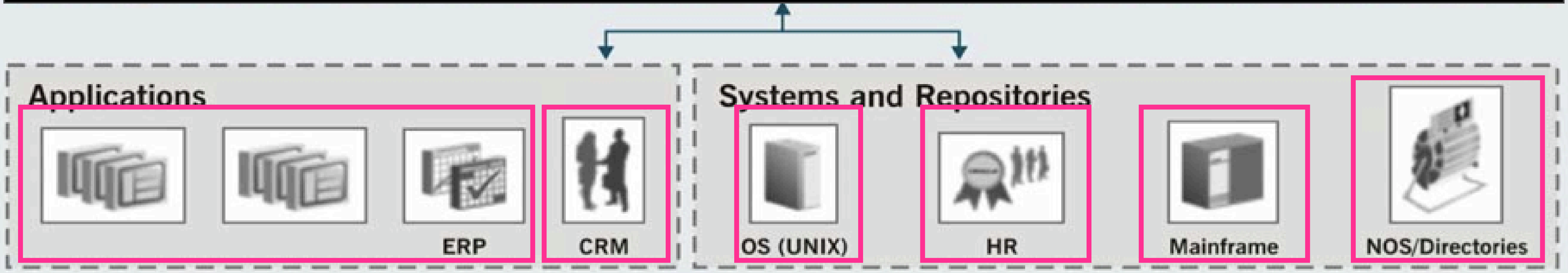
Where is IdM in 2007

- Infrastructure (Commoditized, Strong Standards)
- Middleware (Partially Commoditized, Effective but incomplete technical standards)
- Application (not at all commoditized, weak or nonexistent open standards)

Common Identity Management

- Directory Services
- Access Management
- Identity Administration
- Identity Provisioning

1. IDENTITY SILOS ARE EVERYWHERE.
2. A SINGLE CENTRALIZED DIRECTORY IS NOT FEASIBLE FOR MOST ORGANIZATION.



Applications

ERP

CRM

Systems and Repositories

OS (UNIX)

HR

Mainframe

NOS/Directories

How to deal with Identity Silo

- Directory enabled your applications
- Use Virtual Directory for quick linkage between multiple AUTHORITATIVE identity silos

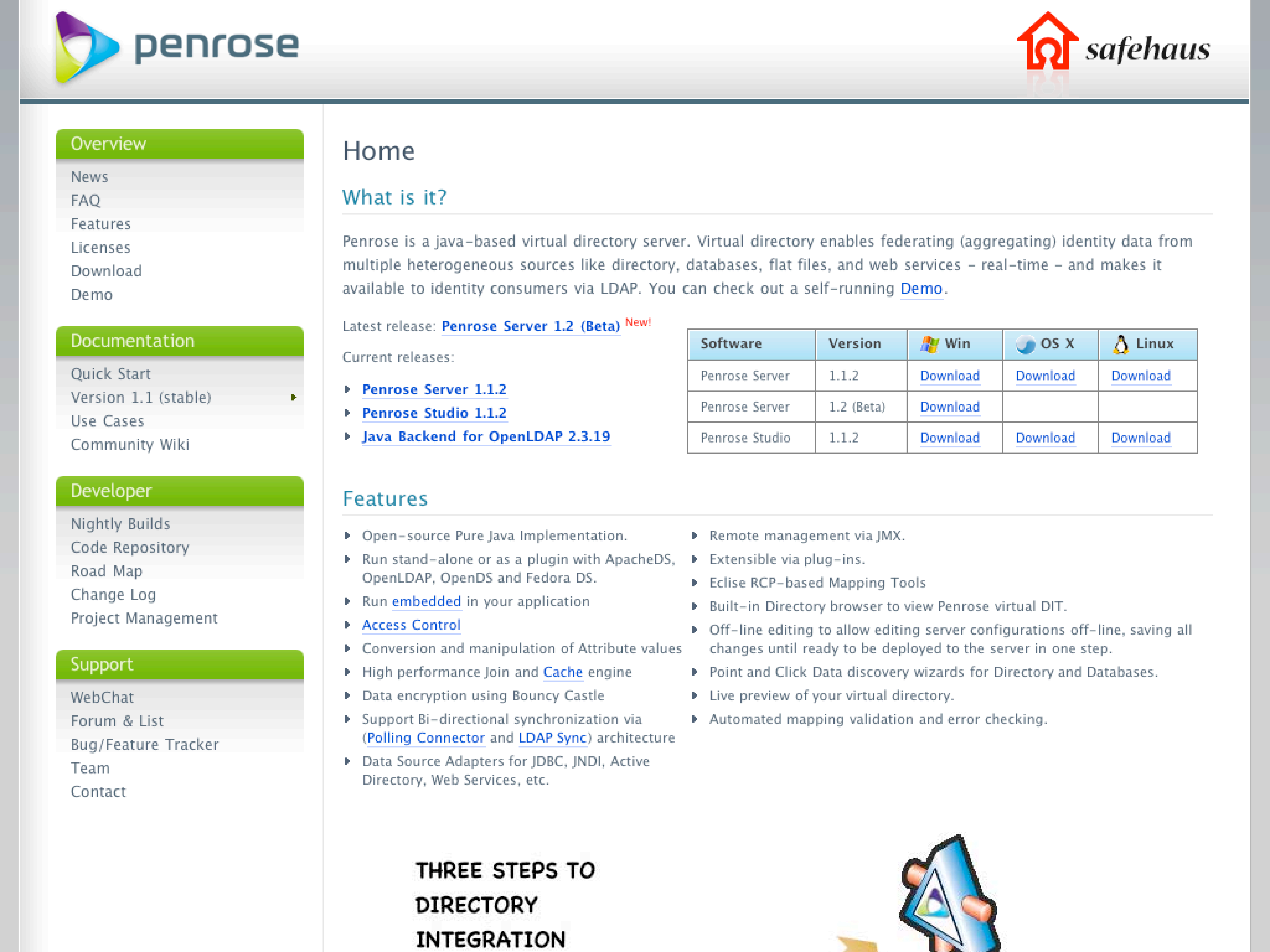
Demo
Virtual Directory

Objectives:

- Join two identities from database (MySQL) and directory (OpenDS) based on common key (username)
- Create MemberOf View in LDAP from users/groups stored in a database

Tools used for Demo

- Database Server: MySQL
- Directory Server: OpenDS
- LDAP Client: LDAP Studio
- MySQL Client: CocoaMySQL
- Penrose Server
- Penrose Studio



Overview

- News
- FAQ
- Features
- Licenses
- Download
- Demo

Documentation

- Quick Start
- Version 1.1 (stable)
- Use Cases
- Community Wiki

Developer

- Nightly Builds
- Code Repository
- Road Map
- Change Log
- Project Management

Support

- WebChat
- Forum & List
- Bug/Feature Tracker
- Team
- Contact

Home

What is it?

Penrose is a java-based virtual directory server. Virtual directory enables federating (aggregating) identity data from multiple heterogeneous sources like directory, databases, flat files, and web services - real-time - and makes it available to identity consumers via LDAP. You can check out a self-running Demo.

Latest release: **Penrose Server 1.2 (Beta)** New!

Current releases:

- **Penrose Server 1.1.2**
- **Penrose Studio 1.1.2**
- **Java Backend for OpenLDAP 2.3.19**

Software	Version	Win	OS X	Linux
Penrose Server	1.1.2	Download	Download	Download
Penrose Server	1.2 (Beta)	Download		
Penrose Studio	1.1.2	Download	Download	Download

Features

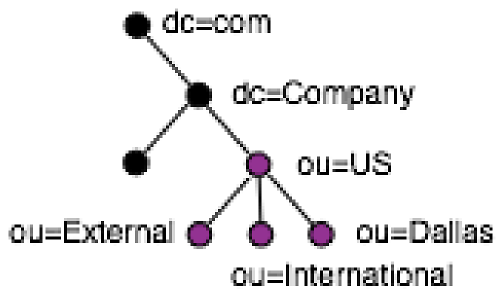
- Open-source Pure Java Implementation.
- Run stand-alone or as a plugin with ApacheDS, OpenLDAP, OpenDS and Fedora DS.
- Run embedded in your application
- Access Control
- Conversion and manipulation of Attribute values
- High performance Join and Cache engine
- Data encryption using Bouncy Castle
- Support Bi-directional synchronization via (Polling Connector and LDAP Sync) architecture
- Data Source Adapters for JDBC, JNDI, Active Directory, Web Services, etc.
- Remote management via JMX.
- Extensible via plug-ins.
- Eclise RCP-based Mapping Tools
- Built-in Directory browser to view Penrose virtual DIT.
- Off-line editing to allow editing server configurations off-line, saving all changes until ready to be deployed to the server in one step.
- Point and Click Data discovery wizards for Directory and Databases.
- Live preview of your virtual directory.
- Automated mapping validation and error checking.

PeopleSoft Portal:

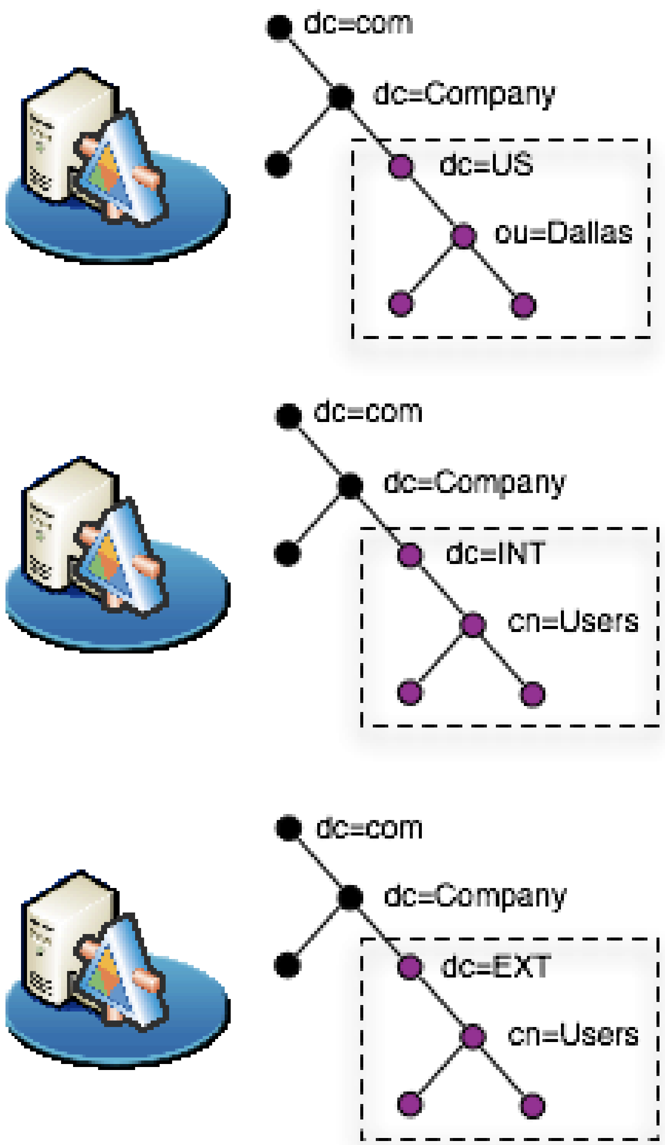
Can only authenticate against one Directory tree with one user search information, i.e: one search base, one scope, one search attribute and one filter

Penrose:

Penrose merges three AD domains/servers into the following virtual tree:



The authentication request from PeopleSoft is "Passed Through" to the corresponding AD server



Access Management

OSS Web-SSO Comparison

	CAS 3.1	OpenSSO	JOSSO 1.5
AuthN Model	Kerberos Style	Agent based *	JAAS *
AuthZ	N/A	Through AM	JAAS
Client Support	√ √ √ √	√ √ √	√ √
Learning Curve	√ √ √	√ √ √ √	√ √ √
User Community	√ √ √ √	√ √	√ √
Interoperability	√ √	√ √ √	√ √
Federation	Support/Non-Standard	SAML 2.0	Support/Non-Standard

OpenSSO Highlight

- Authorization/Policy Service through AM
- Federation via SAML and Liberty Service
- Integrates well with J2EE model

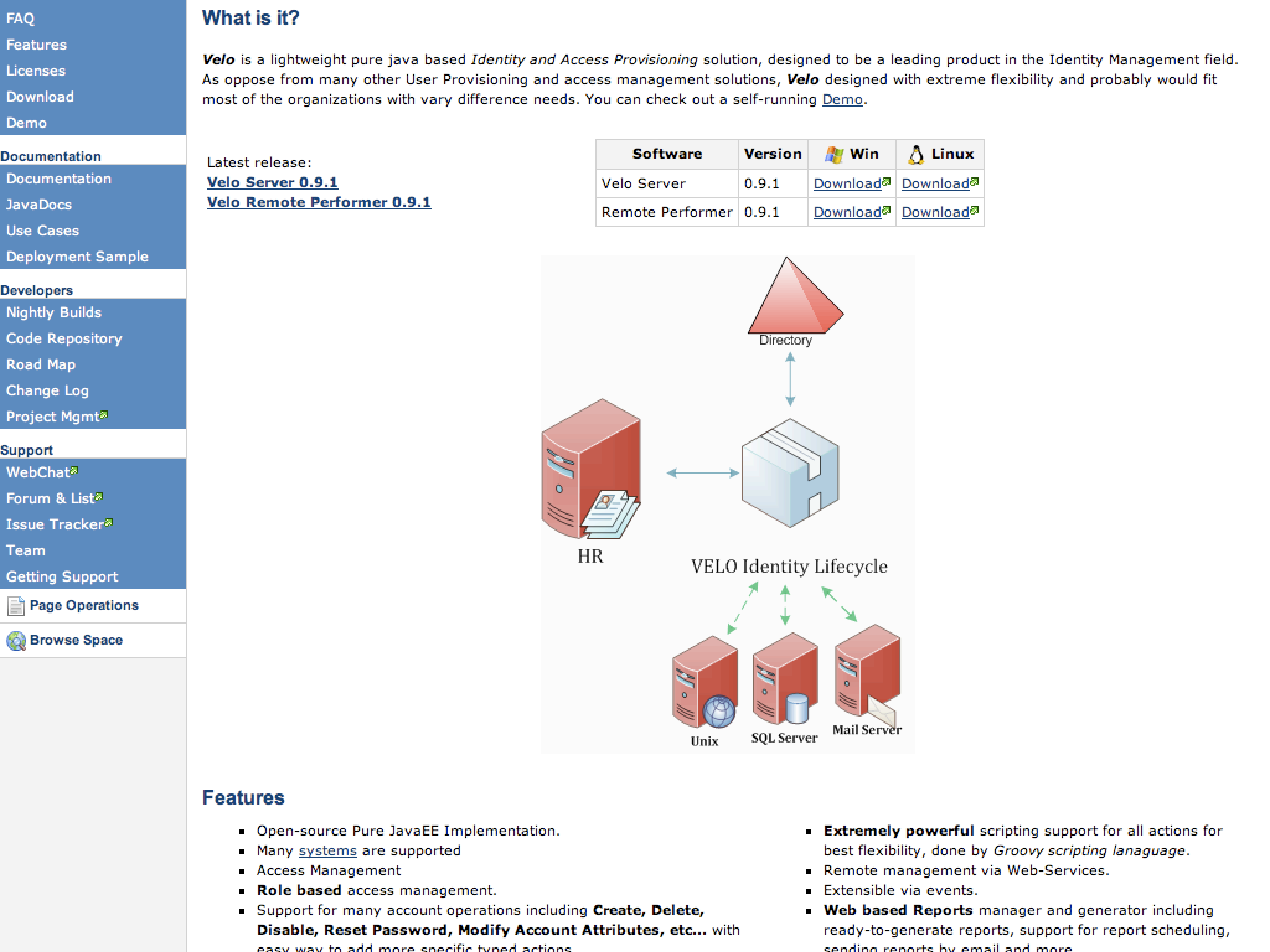
JOSSO Highlight

- Non Intrusive (JOSSO-enabled App has no run-time dependency with JOSSO)
- JAAS-based (Access Control through J2EE)
- Transparent (no proprietary API)
- Handle the authentication flow and leaving user identity accessible via Servlet/EJB
- End-to-end declarative integration with Jboss and tomcat

Provisioning

Core User Provisioning Capabilities

- Connectors Breath
- Delegated Administration (use LDAP Group)
- Self-Service
- HR-Application support



- FAQ
- Features
- Licenses
- Download
- Demo

Documentation

- Documentation
- JavaDocs
- Use Cases
- Deployment Sample

Developers

- Nightly Builds
- Code Repository
- Road Map
- Change Log
- Project Mgmt

Support

- WebChat
- Forum & List
- Issue Tracker
- Team
- Getting Support

Page Operations

Browse Space

What is it?

Velo is a lightweight pure java based *Identity and Access Provisioning* solution, designed to be a leading product in the Identity Management field. As oppose from many other User Provisioning and access management solutions, ***Velo*** designed with extreme flexibility and probably would fit most of the organizations with vary difference needs. You can check out a self-running Demo.

Latest release:
Velo Server 0.9.1
Velo Remote Performer 0.9.1

Software	Version	Win	Linux
Velo Server	0.9.1	Download	Download
Remote Performer	0.9.1	Download	Download

Features

- Open-source Pure JavaEE Implementation.
- Many systems are supported
- Access Management
- **Role based** access management.
- Support for many account operations including **Create, Delete, Disable, Reset Password, Modify Account Attributes, etc...** with easy way to add more specific typed actions.
- **Extremely powerful** scripting support for all actions for best flexibility, done by *Groovy scripting lanaguage*.
- Remote management via Web-Services.
- Extensible via events.
- **Web based Reports** manager and generator including ready-to-generate reports, support for report scheduling, sending reports by email and more.

Join Conversation at

http://groups.google.com/group/safehaus