AXIOMATICS POLICY SERVER

The Axiomatics Policy Server is the industry-leading solution to control access to critical applications. Using externalized dynamic authorization, it provides the most efficient policy engine on the market, and the most complete solution available for enterprise-wide roll out of Policy and Attribute Based Access Control (PBAC and ABAC).

The Axiomatics Policy Server (APS) provides a complete authorization infrastructure that scales with the demands of the enterprise. Its dynamic authorization capabilities have been designed to address the access-control needs of a broad range of systems and organizations.

AXIOMATICS POLICY SERVER MAIN COMPONENTS

At the core is an authorization engine, a service that evaluates eXtensible Access Control Markup Language (XACML) 3.0 policies. This is available in two form factors:

- **Access Decision Service (ADS)**, a cloud-native authorization engine suitable for flexible deployment in microservices, cloud or hybrid architectures
- **Policy Decision Point (PDP)**, a web application-based authorization engine managed by Axiomatics Services Manager (ASM)

Additional services can be provided by Axiomatics Reverse Query engine, which is used to compute the conditions that need to be satisfied to reach a desired authorization decision; which can also be exposed as SQL SELECT statements. The services ARQ Raw and ARQ SQL are both managed by Axiomatics Services Manager (ASM) as part of the PDP, but subject to their own licensing. Authorization services all share the same set of policies and configurations and are managed in authorization domains.

SUPPORTING TOOLS AND COMPONENTS

Management Tools

- **The Axiomatics Services Manager (ASM)** is included in a standard APS installation. It is a web-based management console that allows administrators to manage services, domains, and resources from a central point.
- **Attribute connectors** are the means to retrieve attributes from data sources such as LDAP directories and SQL databases; custom attribute connectors can be developed to access other data sources.
- **The Attribute Dictionary,** also managed in ASM, allows the user to define, organize and use XACML attributes. An attribute is uniquely identified by a particular combination of ID, name, namespace, category, and data type. These attributes can be used when creating policies in the policy authoring tools.

SUPPORTING TOOLS AND COMPONENTS, CONTINUED

Authoring Tools

- **A Policy Editor** with a graphical user interface is built into Axiomatics Services Manager to simplify policy creation and maintenance.

- Text-based policy editing can be done using **Axiomatics Language for Authorization (ALFA)**. This is an Eclipse plugin that turns your IDE (integrated development environment) into an XACML policy programming tool, and a CLI (command line interface) compiler tool that can be used to create policy packages.

Testing, Analysis, and Reporting Tools

- **Axiomatics Policy Auditor (APA)** is a web-based tool that can be used to verify XACML policies. The APA application can be installed as a standalone application or integrated with Axiomatics Policy Server (APS).

- **Axiomatics Review Manager (ARM)** is a tool for performing access reviews, that is, reviews verifying that permissions are correct and access control settings are working as intended.
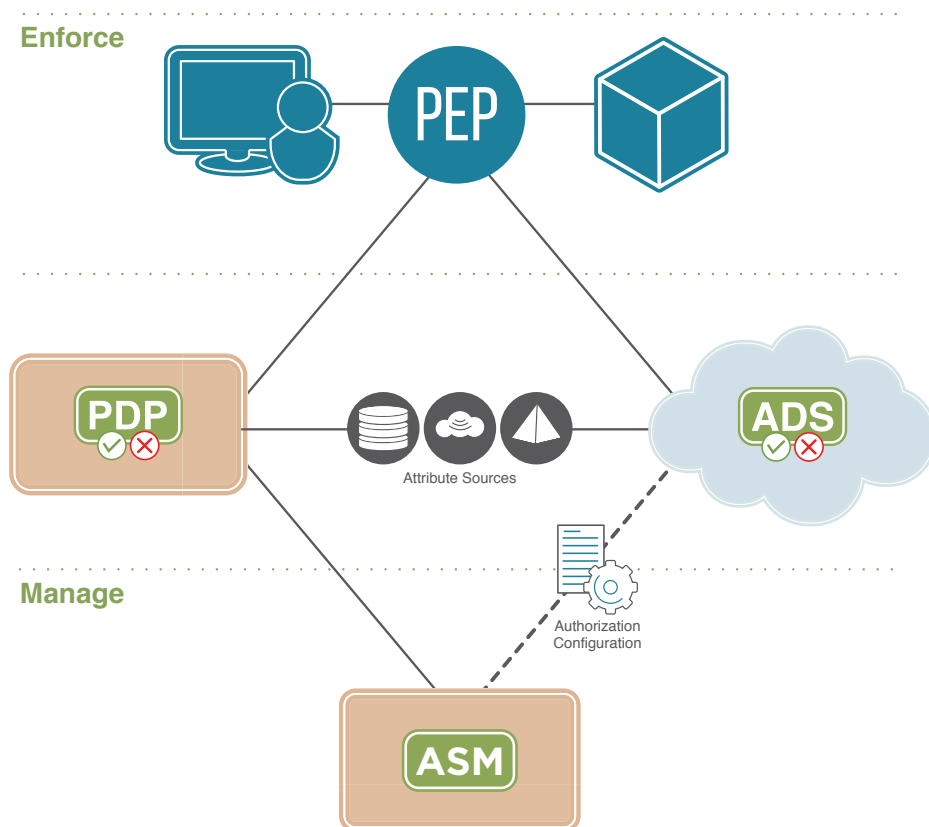
Enforce: The user requests access to an application, which is intercepted by a Policy Enforcement Point (PEP). In this example, we are using a single PEP and a single application - in enterprise-wide deployments, some enterprises choose to use multiple PEPs to serve different types of applications.

Decide: The PEP sends the request to the decision point, either the on-premise Policy Decision Point (PDP) or the cloud native PDP (the component is called the Access Decision Service, or ADS). From there, the PDP applies the policies, providing a permit/deny, based on the authorization configuration (fetched from either ASM or from a cloud store), and attribute sources, which can be anything from an LDAP, active directory, a database, identity attributes, etc.

Manage: The configuration for the decision point and the authorization policies are created and stored in ASM. ASM also directly manages the on-premises PDP services. The cloud native PDP services are designed for flexible deployment in different cloud configurations and not managed by ASM.

OPERATING SYSTEMS

Axiomatics Policy Server is built on top of the Java Virtual Machine and should be expected to run on any platform for which an official, production-ready release of the appropriate Java Virtual Machine exists. Some components may have further requirements.

AUTHORIZATION ENGINES

Access Decision Service (ADS): A cloud native authorization engine, implementing a service that evaluates XACML 3.0 policies.

- Requires Oracle 64-bit Java 8 or Java 11, or OpenJDK 64-bit Java 8 or Java 11
- Client access protocol: REST
- 512 MB memory minimum

Policy Decision Point (PDP): A web application-based authorization engine, managed by Axiomatics Services Manager (ASM), implementing three services:

PDP: a service that evaluates XACML 3.0 policies

- Client access protocol: SOAP and REST
- 2 GB memory minimum

ARQ Raw: a service that is used to compute the conditions that need to be satisfied to reach a desired authorization decision

- Client access protocol: SOAP

ARQ SQL: a service that exposes ARQ Raw results as SQL SELECT statements

- Client access protocol: SOAP

Authorization engine attribute retrieval:

- Any LDAP v3 compliant directory
- Any JDBC 4 compliant SQL database
- Easy-to-use API facilitates development of custom attribute retrieval components for any data source

POLICY ENFORCEMENT POINTS

Policy Enforcement Points (PEPs) for a broad variety of environments and applications can be created using REST or SOAP APIs, or PEP SDKs for Java and .NET.

POLICY AUTHORING

- A Policy Editor with a graphical user interface is built into ASM
- Text-based policy editing can be done using Axiomatics Language for Authorization (ALFA). Requires Java 8 and the Eclipse IDE.

POLICY ANALYSIS AND REPORTING

- **Axiomatics Policy Auditor (APA) ca**n be installed as a standalone application or integrated with Axiomatics Policy Server (APS). A standalone installation requires Oracle Java Runtime Environment (JRE), version 6 Update 21, or higher.

- **Axiomatics Review Manager (ARM)** is a web application that runs in a servlet container or application server using a SQL database for data storage. See requirements for Apache Tomcat and IBM WebSphere below.

AUTHORIZATION ENGINES MANAGEMENT

Axiomatics Services Manager (ASM) is a management component within the Axiomatics authorization system, which is used to manage the web application-based authorization engines.

General Requirements

- x86-64 CPU
- 4 GB memory recommended

Client Access Protocol

- SOAP

Application Server, Java Versions, and Web Services Stacks

- Apache Tomcat 7, 8, 8.5, and 9, Oracle 64-bit Java SE 7 and 8, Metro Web Services Stack 2.3
- 64-bit IBM WebSphere Application Server (WAS) or WAS ND 8.0 (with IBM Java 6) or 8.5 (with IBM Java 6, 7 or 8), or 9.0 (with Java 8)
- Red Hat JBoss EAP 6.4, Oracle 64-bit Java SE 8

Supported Browsers

- Firefox 42.x or later
- Chrome 46.x or later
- IE 11, with latest updates
- Edge 40.x or later

Databases for ASM Configurations

- Oracle 11g and 12c
- SQL Server 2008, 2012, 2014, and 2016
- PostgreSQL 9
- IBM DB2 (LUW) 9.7, 10.1, and 10.5