AccessMatrix™ UAM

企业应用系统的通用安全平台

Web访问管理，联邦SSO和授权模型管理

关键优势

- 便于集成和部署现有 LDAP、AD 和 JDBC 目录，无需修改现有建设方案与用户存储体系
- 提供了一个可扩展的，开放的和可靠的平台来支持运营要求，如自动故障转移，水平垂直扩展和 7x24 全天候运营
- 提供安全管理和4A服务实施，包括认证策略，认证方式，用户存储和管理委托授权，以及审计合规性报告
- 采用身份和访问管理解决方案，为企业与互联网应用访问提供IAM服务，降低集成和运营成本

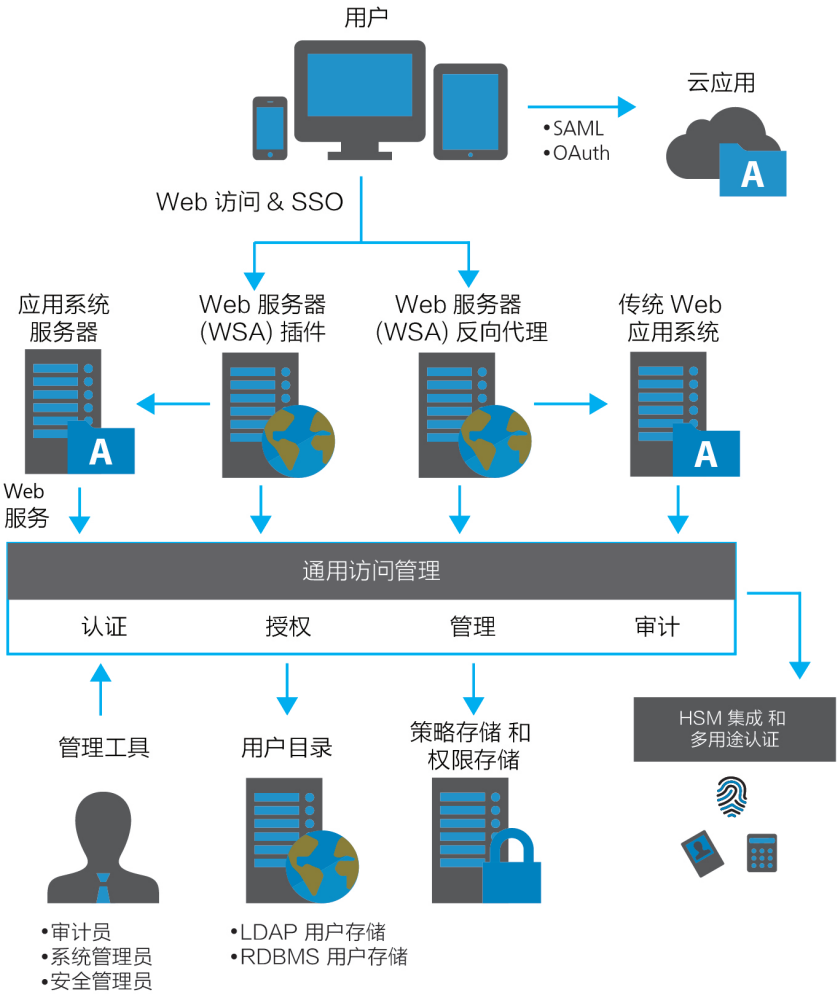
AccessMatrix™ 通用访问管理（Universal Access Management，UAM）是一个综合的 Web 单点登录，Web 访问控制管理，联合单点登录，外部授权管理和分层授权的管理系统。利用 AccessMatrix™ 专利技术，UAM 为企业业务应用提供安全管理、认证、授权和审计服务（4A）全方位防护；保障企业应用安全符合最高标准要求。UAM 是基于金融行业合规性要求和标准创建，因此 UAM 可为企业应用系统和互联网应用程序定制通用的身份和访问管理（IAM）服务，并降低集成成本。

UAM 可提供无缝集成的 Web 访问管理方式，来实现基于 Web 的应用系统的单点登录。除此之外，对于云应用，特别是采用分布式部署架构的应用体系，可以采用基于 SAML 标准的低耦合联邦的单点登录方法。

UAM 是为保护多层次应用系统安全而设计的，无论是基于 Web 还是非 Web 的应用，亦或是运行在企业数据中心或云端的应用系统。通过 Web 安全代理（WSA）来拦截 Web 请求，UAM都可以根据由安全管理员定义的集中访问控制策略来保护 Web 应用系统和应用服务器免受由 OWASP 发布的威胁。

减少业务应用系统开发人员在为符合复杂的安全、审计以及合规性监管要求方面投入的研究与学习时间；UAM 提供了一整套完整即用的开发工具包；从而提升了企业的生产效率，降低了开发成本。

采用具有专利权的分层分区的安全管理和授权框架，UAM 已经被证实完全满足对区域/部门应用系统、银行对公业务应用系统、管理安全供应商和 SaaS 供应商的管理需求。



特点

- 内置强身份认证，Web 单点登录，联邦单点登录和企业单点登录可运行在同一后台
- 可扩展的插入式认证模块支持采用短信，硬件和软件令牌的强身份认证需求
- 灵活和开放的 API 提供便于集成和代码重用的安全4A服务
- 防篡改审计跟踪日志
- 可扩展性

系统要求

- 服务器 OS: MS Windows Server 2008、IBM AIX、Oracle Linux、Oracle Solaris
- 应用服务器: Oracle WebLogic、IBM WebSphere 和 Apache Tomcat
- Java 运行环境: JRE 1.6 及以上
- 数据库支持: MS SQL Server、Oracle RDBMS、IBM DB2 和 Oracle MySQL
- 外部用户存储: AD目录、LDAP v3 兼容目录 和 JDBC 兼容数据库
- FIPS 认证的 HSM

应用集成

- 提供灵活开放的安全的 4A 服务API提供快速的的代码集成和重用。UAM API 支持各种编程语言的 Web 服务，Java 和 .NET 接口。
- 采用适用于现有主流 Web 和应用服务器的 Web 安全代理插件，可支持 Web 应用的 URL 级访问控制，并通过标准 HTTP 响应头推送用户信息以协助 Web 应用建立用户身份和集合多个目录的信息。
- 与外部用户存储的无缝集成（如 LDAP、AD 目录、JDBC），企业可直接使用现有用户注册表无需同步用户信息。 UAM 服务器可以访问外部用户存储目录，以简化集成工作。

可拓展性

可靠性和可扩展性的设计，UAM 利用商业级的 Java 应用服务器（如 IBM 的 Websphere，Oracle 的 WebLogic ）来支持高可用性，水平垂直扩展和 7x24 全天候运维。 UAM 通过其事件监听器 SDK 或建立队列机制（如 IBM MQ），来支持可扩展，无中断运行。 UAM 拥有多达1千万个用户生产系统。

身份认证

- 灵活的安全密码策略和质量检查是由内置的密码控制模块和 LDAP 认证模块来支持。支持增强的 HSM 的端到端加密。
- 可扩展的插入式认证模块（PAM）支持采用 SMS、 硬件和软件令牌的强身份认证请求。包括：Vasco、Gemalto、SafeNet、OATH 等。

外部授权

- 内置基于角色的访问控制 (RBAC) 模块授予用户或组特定的应用角色。成功授权后，可通过 HTTP Header 或网络服务，将用户角色信息传递给应用。
- 把在不同应用系统中的用户ID通过用户授权映射（User Authorization Mapping）映射到同一个SSO ID，这是一个把现有应用迁移到 UAM SSO 系统上的非常有效的共存策略。这样不同系统间就即可使用达成一致的契约/策略来完成凭证和数据的交互。

管理

- 授权和管理范围由基于 Web 管理控制台定义。安全管理功能可限定在某个特定的用户存储区的某个特定组织机构或区段（例如 AD 目录）。管理权限可由 Root 管理员委托授权给其下级管理员，以提高安全，明确安全管理职责。该框架允许外部组织（如客户和业务合作伙伴）通过他们自己的安全管理员使用定制接口来管理企业用户的 ID 和用户权限。
- 最佳安全实践，例如通过在 SafeNet 和 Thales 中建立 HSMs（硬件安全模块）进行密钥管理，UAM 可以在管理控制台强制实施，如双重控制工作流、最少权限和有限的责任划分等措施，进行更改安全策略和其他关键操作。

审计

- 防篡改审计跟踪日志来满足管理、访问、和交易审计的需求。除了标准的审计跟踪日志外，UAM 审计 API 可以用来生成特定的审计跟踪信息。
- 审计报告模块提供一套标准的以用户为中心的报告功能，来报告管理和访问活动。报告可以用 Jasper 通过 SQL 视图便于进行定制。

北京安讯奔科技有限责任公司
北京市海淀区西直门北大街60号
首钢国际大厦1509室100082
咨询热线：0756-6322666
www.axbsec.com

安讯奔分公司和办事处
珠海-成都-上海-深圳-广州