## 一、平台背景

随着信息技术的不断发展和信息化建设的不断进步，业务应用、办公系统、商务平台不断推出和投入运行，信息系统在企业的运营中全面渗透。电信行业、财政、税务、公安、金融、电力、石油、大中型企业和门户网站，使用数量众多的网络设备、服务器主机来提供基础网络服务、运行关键业务，提供电子商务、数据库应用、ERP和协同工作群件等服务。由于设备和服务器众多，系统管理员压力太大等因素，越权访问、误操作、滥用、恶意破坏等情况时有发生，这严重影响企业的经济运行效能，并对企业声誉造成重大影响。另外黑客的恶意访问也有可能获取系统权限，闯入部门或企业内部网络，造成不可估量的损失。如何提高系统运维管理水平，跟踪服务器上用户的操作行为，防止黑客的入侵和破坏，提供控制和审计依据，降低运维成本，满足相关标准要求，越来越成为企业关心的问题。

2002年由美国总统布什签发的萨班斯法案(Sarbanes-Oxley Act)开始生效。其中要求企业的经营活动，企业管理、项目和投资等，都要有控制和审计手段。因此，管理人员需要有有效的技术手段和专业的技术工具和安全产品按照行业的标准来做细粒度的管理，真正做到对于内部网络的严格管理，可以控制、限制和追踪用户的行为，判定用户的行为是否对企业内部网络的安全运行带来威胁。

2007年，由公安部、国家保密局、国家密码管理局、国务院信息工作办公室四部门联合印发了《信息安全等级保护管理办法》，为我国信息系统等级保护工作的迅速展开起到了有力的促进作用。配合该《管理办法》的发布，一系列相关国家标准也进入紧锣密鼓的制定和审批当中。如：《信息系统安全等级保护基本要求》（以下简称《基本要求》）、《信息系统安全等级保护-定级指南》、《信息系统安全等级保护-实施指南》、《信息系统安全等级保护-测评准则》等。其中《基本要求》针对每个等级的信息系统提出相应安全保护要求，按照《基本要求》进行保护后，信息系统达到一种相对安全的状态，即具备了相应等级的信息安全保护能力

## 二、概念介绍

4A (认证Authentication、账号Account、授权Authorization、审计Audit)统一安全管理平台解决方案。

1995年，国际网安界最早提出4A(认证Authentication、账号Account、授权Authorization、审计Audit)统一安全管理平台解决方案概念，正式将身份认证作为整个网络安全的基础及不可或缺的组成部分，即将身份认证、授权、审计和账号（即不可否认性及数据完整性）定义为网络安全的四大组成部分，从而确立了身份认证在整个网络安全系统中的地位与作用。

所谓4A统一安全管理平台解决方案，即融合统一用户账号管理、统一认证管理、统一授权管理和统一安全审计四要素后的解决方案将涵盖单点登录（SSO）等安全功能，既能够为客户提供功能完善的、[高安](http://baike.baidu.com/view/245652.htm)全级别的4A管理，也能够为用户提供符合萨班斯法案（SOX）要求的[内控](http://baike.baidu.com/view/460936.htm)报表。

## 三、功能概述

### 1. 集中帐号(account)管理

为用户提供统一集中的帐号管理，支持管理的资源包括主流的操作系统、网络设备和应用系统；不仅能够实现被管理资源帐号的创建、删除及同步等帐号管理生命周期所包含的基本功能，而且也可以通过平台进行帐号密码策略，密码强度、生存周期的设定。

### 2. 集中认证(authentication)管理

可以根据用户应用的实际需要，为用户提供不同强度的认证方式，既可以保持原有的静态口令方式，又可以提供具有双因子认证方式的高强度认证（一次性口令、数字证书、动态口令），而且还能够集成现有其它如生物特征等新型的认证方式。不仅可以实现用户认证的统一管理，并且能够为用户提供统一的认证门户，实现企业信息资源访问的单点登录。

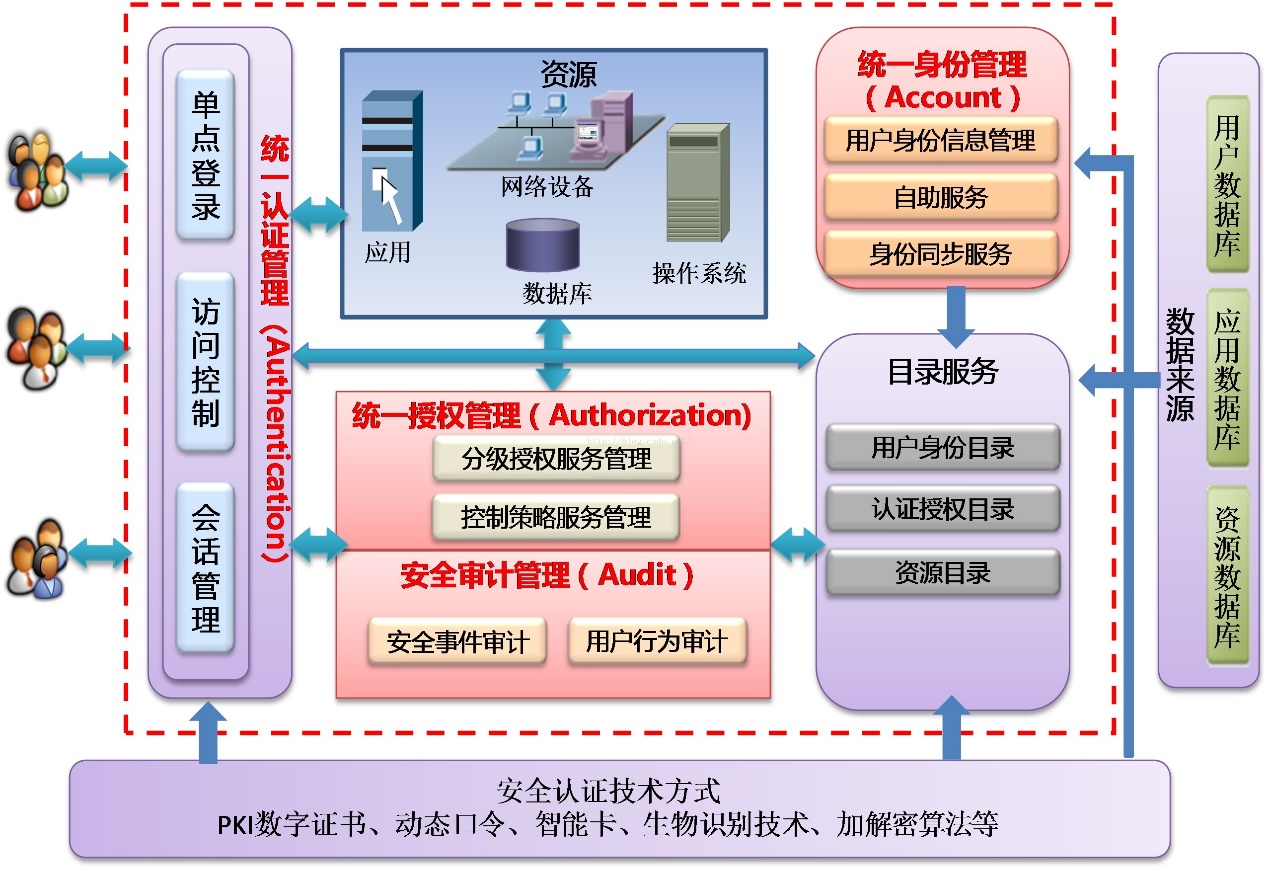
### 3. 集中权限(authorization)管理

可以对用户的资源访问权限进行集中控制。它既可以实现对B/S、C/S应用系统资源的访问权限控制，也可以实现对数据库、主机及网络设备的操作的权限控制，资源控制类型既包括B/S的URL、C/S的功能模块，也包括数据库的数据、记录及主机、网络设备的操作命令、IP地址及端口。

### 4. 集中审计(audit)管理

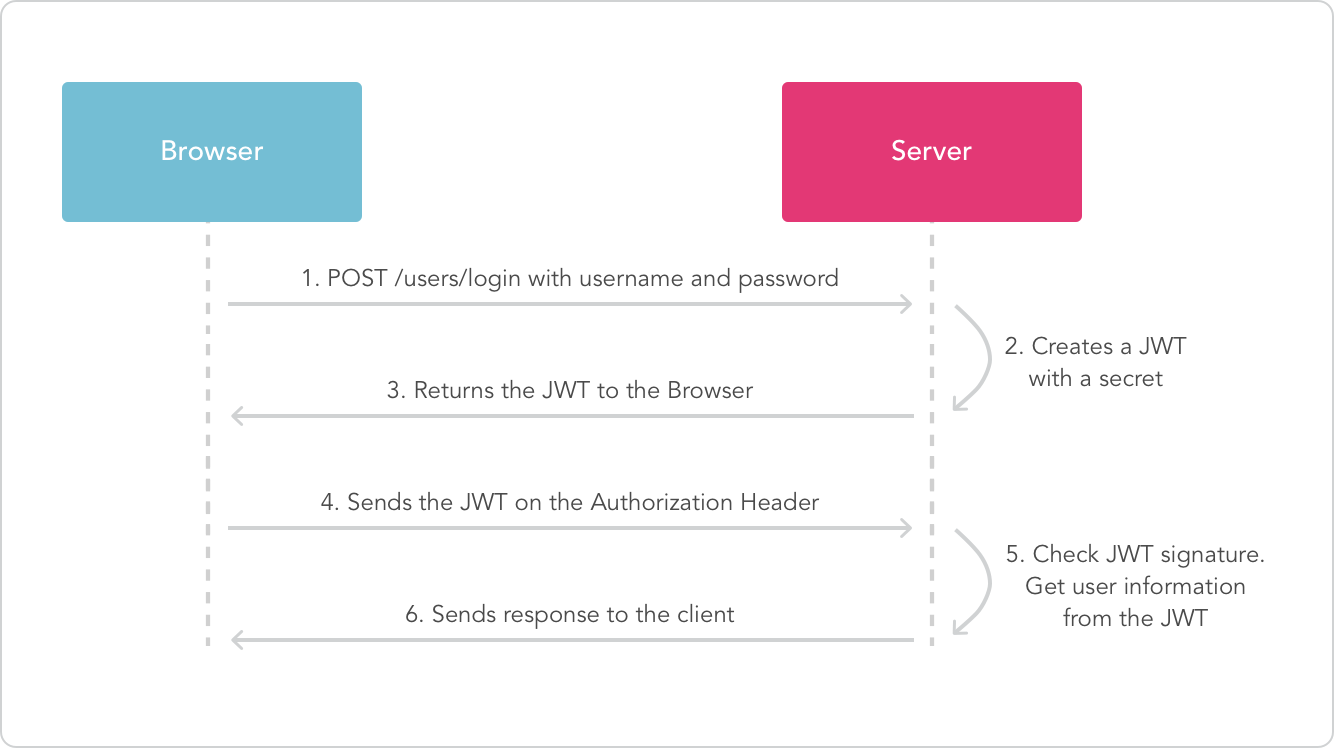
将用户所有的操作日志集中记录管理和分析，不仅可以对用户行为进行监控，并且可以通过集中的审计数据进行数据挖掘，以便于事后的安全事故责任的认定。

## 四、平台设计



## 五、技术选型

JWT认证流程



未完待续……