DOI: 10.19666/j.rlfd.202212109

基于零信任架构的集团级 AAA 系统设计与实现

肖力炀，毕玉冰，刘 骁，朱博迪，刘 迪，刘超飞，崔逸群
（西安热工研究院有限公司，陕西 西安 710054）

［摘 要］为了解决目前集团信息系统中普遍存在的用户账号管理与安全防护的问题，提出了一种基于零信任架构的集账号、认证和审计于一体的 AAA 系统。首先，对 AAA 系统的用户管理、身份认证授权、用户审计等模块进行功能描述；然后，针对传统网络边界防护问题，采用基于零信任架构的认证授权方式对业务场景进行身份鉴别，以保障业务系统环境的可靠性；最后，对 AAA 子系统的逻辑及集团级系统开发平台配置进行说明。提出的 AAA 系统可有效提高集团级企业信息系统的业务安全，弥补零信任环境下用户登录账号的安全问题，也进一步提高了集团级企业内网络设备、应用设备、系统和应用管理的安全防护能力。

［关 键 词］零信任；身份认证；账号安全；认证授权；网络安全

［引用本文格式］肖力炀，毕玉冰，刘骁，等. 基于零信任架构的集团级 AAA 系统设计与实现[J]. 热力发电，2023，52(9)：171-180. XIAO Liyang, BI Yubing, LIU Xiao, et al. Group-level AAA system design and implementation based on zero trust architecture[J]. Thermal Power Generation, 2023, 52(9): 171-180.

Group-level AAA system design and implementation based on zero trust architecture

XIAO Liyang, BI Yubing, LIU Xiao, ZHU Bodi, LIU Di, LIU Chaofei, CUI Yiqun
(Xi'an Thermal Power Research Institute Co., Ltd., Xi'an 710054, China)

Abstract: In order to solve the problems of user account management and security protection in current group information system, this paper proposes a three-in-one AAA system of account, authentication and audit based on zero-trust architecture. Firstly, it describes the function of user management, authentication authorization, user audit and other modules of the AAA system. Secondly, in view of the conventional network boundary protection problem, the authentication authorization method based on zero trust architecture is applied to identify the business scenario, thus to ensure the reliability of the business system environment. Lastly, it illustrates the logic of the AAA subsystem and group-level system development platform configuration. The proposed AAA system can effectively improve the business security of group-level enterprise information system, compensate for the security issues of user login account under zero-trust environment, and further improve the security protection ability of network equipment, application equipment, system and application management in group-level enterprise.

Key words: zero trust; identity authentication; account security; certification authorization; cyber security

随着一些大型集团公司应用系统数量和用户的不断增加，员工因业务需要而使用多个应用系统的情况也越来越多，异构系统、融合网络、多样设备的用户身份管理复杂度也达到前所未有的程度，弱口令、僵尸账户、冗余账户、账号冒用、钓鱼用户、重复登录、异地登录、异常登录、多样性访问、分散管理、审计弱化等网络安全问题层出不穷。因此，从安全角度来说，构建集团内全网络、全应用、全覆盖的统一用户身份管理系统，保障用户身份与账号在企业中的唯一性显得尤为重要[1-3]。

近年来，随着工业互联网和企业数字化的不断发展，以云计算、人工智能、大数据技术等为支撑

修 回 日 期：2022-12-10
基 金 项 目：中国华能集团有限公司总部科技项目（HNKJ21-H29）
Supported by: Science and Technology Project of China Huaneng Group Co., Ltd. (HNKJ21-H29)
第一作者简介：肖力炀（1996），女，硕士，助理工程师，主要研究方向为网络安全与信息安全，xiaoliyang@tpri.com.cn。

的信息系统日益增多，内外网络防护的安全边界也逐渐趋于模糊化，许多企业基于边界防护的网络安全架构难以应付身份、权限、系统漏洞等维度的攻击，安全架构亟需升级。传统的网络架构通常被划分为外网、内网和“隔离区”（demilitarized zone，DMZ）等不同安全区域，并采用基于网络边界防护的方案，通过在网络的边界处部署防火墙、虚拟专用网络（virtual private network，VPN）、Web 应用防护系统（Web application firewall，WAF）等技术进行防护。但这种架构会存在“防外不防内”的问题，即默认内网更安全，对内网中的系统和设备完全信任，因此攻击者只要通过一些攻击手段绕过网络边界防护，渗透到企业内网中，内网安全就会轻易被瓦解，从而造成企业数据泄露问题[4-6]。

2010 年 John Kindervag 首次提出了零信任的概念[7-8]，认为“可信”的内部网络充满着威胁，“信任”被过度滥用。针对传统网络边界防护带来的弊端，零信任给出了一种“从来不信任，始终被校验”的思想，即不信任网络内外的任何用户、设备、系统与应用，而是通过动态认证和授权的方式处理每一个访问请求，确保在持续访问过程中验证和评估真实访问上下文和访问预期的偏差，避免非法用户拿到合法授权[9-12]。这种方式使网络安全架构从网络中心化逐渐走向身份中心化，通过身份认证来实现对设备及系统的访问控制。2017 年谷歌耗时 6 年开发的 Beyond Corp 项目[13-14]，通过引入零信任网络架构模式，消除了对网络信任的依赖，也使零信任网络逐渐被各大企业认可和普及[15-16]。2020 年万振楠等[17]提出了一种边云一体化的身份认证平台，采用基于零信任思想的静态口令与 CA 数字证书相结合的方式，开发出一套用户身份认证平台并投入使用。2021 年李崇智等[18]为解决多个系统之间用户权限分散的问题，提出了一种基于零信任架构的统一身份认证平台，采用身份与设备的动态认证，实现了更为精细化的权限控制。

基于以上研究现状，目前企业信息系统中账号管理仍然面临一些问题：1）存在大量的占用账户、长期不用账号（僵尸账号）、多次创建的冗余账户等，系统管理员梳理起来较为困难；2）账号缺乏统一集中管理，应用系统、VPN、网络准入等缺乏统一的账号管理标准；3）缺乏统一的认证，VPN、各应用系统、APP 认证各自独立，存在大量的弱口令；4）缺乏统一的审计能力，现有业务系统审计日志过多，审计人员有限，无法有效落地审计能力。因此，本文提出了一种基于零信任架构的集账号（account）、认证（authentication）与审计（audit）三位一体的 AAA 系统，进一步提高大型集团公司账号身份的认证管理与安全防护能力。

1 AAA 系统介绍

1.1 基于零信任架构的集团级系统介绍

零信任网络架构的核心思想包括：1）网络无时无刻不处于危险之中；2）网络始终存在内部威胁和外部威胁；3）网络位置不能决定网络访问的可信程度；4）所有设备和网络流量都需要通过认证和授权；5）安全策略是动态且可调整的，或是通过多源信任评估得到的。

传统的企业信息管理系统属于孤岛式作业平台，即一套业务逻辑配合一套管理人员，每套系统都有单独的账号和密码，不同系统之间账号和数据互不相通，导致运维管理较为复杂。为了更好地解决集团级企业内，即多层下属单位各种信息系统之间应用账号的管理与安全问题，建立一站式作业平台，实现应用系统及其他资源的统一认证与管理，本文引入零信任思想，并在此基础上设计了一种集账号、认证、审计功能为一体的 AAA 系统（图 1）。

AAA 系统具备以下 3 种能力：1）集团级全网集中的账号管理能力，可对全网账号进行集中化、标准化和可视化的管理；2）集团级全网统一的认证能力，可对全网人员和业务认证提供标准化和服务化管理；3）集团级全网统一的审计能力，提升审计能力并落地审计管理，实现真正的有效审计。图 1 中，系统核心功能为用户管理、身份认证管理、审计管理等。

1.2 系统架构

图 2 为基于零信任的 AAA 系统整体架构，共分为 6 层，分别是数据层、业务层、中间层、服务层、接口层和展示层。图 2 的展示层提供管理员和普通用户统一登录页面，并提供普通用户单点访问应用系统页面和管理员管理 AAA 系统的配置页面。接口层实现前端展示层与后端业务层的业务交互，除了对内提供接口调用，还可对外提供标准接口对接，通过接口层实现前后端分离，基于每个业务提供单独的业务库。业务层提供 AAA 系统业务管理功能，包括用户管理、认证管理、授权管理和审计管理等。

中间层提供中间件服务和缓存服务，用于业务层与服务层之间交互。服务层提供后台服务，如配置服务、任务调度服务、升级服务、主备服务等。数据层提供业务数据和审计数据存储功能，各业务数据对应各自的业务库，数据之间不能直接访问，都需要通过业务层和接口层交互。

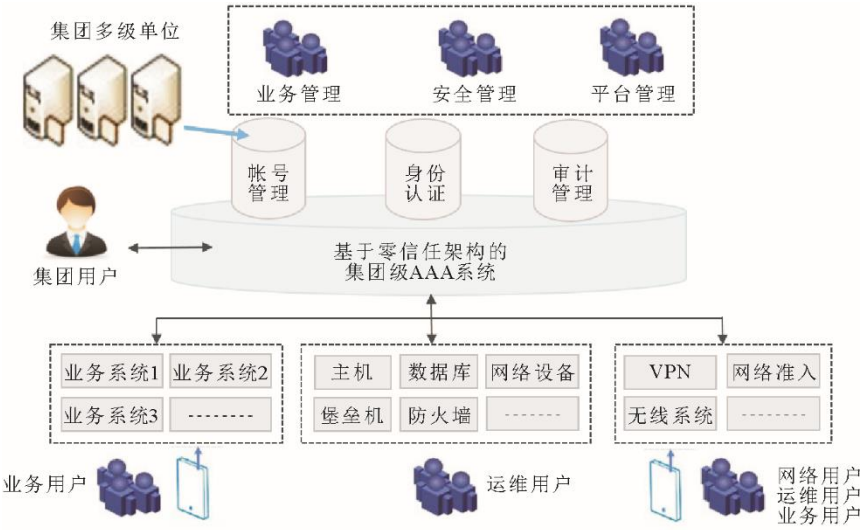


图 1 AAA 系统业务设计
Fig.1 Business design diagram of the AAA system

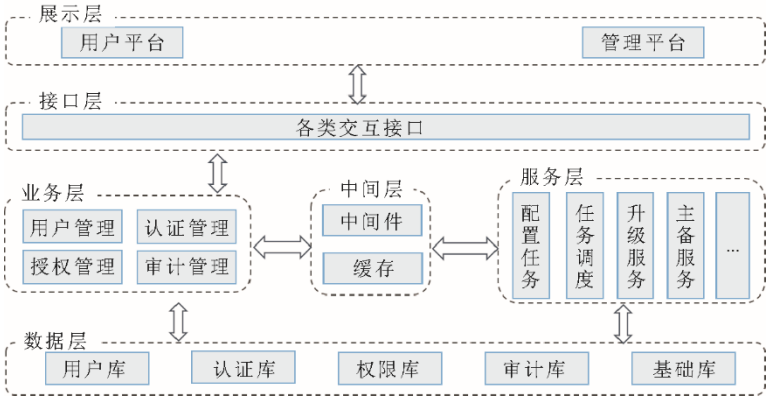


图 2 AAA 系统整体架构
Fig.2 Overall structure of the AAA system

1.3 用户管理

用户管理模块用来实现对用户账号的统一管理，通过同步、映射、关联等方案，形成用户统一登录身份，并对用户属性进行扩展。

图 3 为用户管理模块示意。由图 3 可见：用户管理模块包含了用户的属性管理、用户口令策略、用户状态核查、用户信息同步等子功能；同时支持账号特殊状态管理，包括长期未用账号管理、异常时间登陆账号管理、异地登录账号管理、异地同时登录账号管理等。

1.4 身份认证管理

用户身份认证管理是基于零信任架构的 AAA 系统的核心功能[19-23]。AAA 系统需要通过支持标准协议实现如网络设备、安全设备、主机、应用等资源的统一认证功能，同时还要支持多种强身份认证方式，可以实现多种认证因子的身份认证、票据管理、认证转发，并基于 Radius、LDAP、CAS、OAuth2、OIDC、JWT 等多种标准协议。

认证授权管理功能包括认证和授权 2 个部分。认证管理可通过可信 API 与内部其他业务模块进行交互，同时可与外部认证系统对接实现多种认证方式，通过标准认证协议实现资源认证接入。AAA 系统提供认证服务的同时，还需要根据访问授权控制用户访问资源的权限，只有当用户授予了资源的访问权限，才能进行正常登录，否则即便认证通过，也无法对资源进行登录访问。

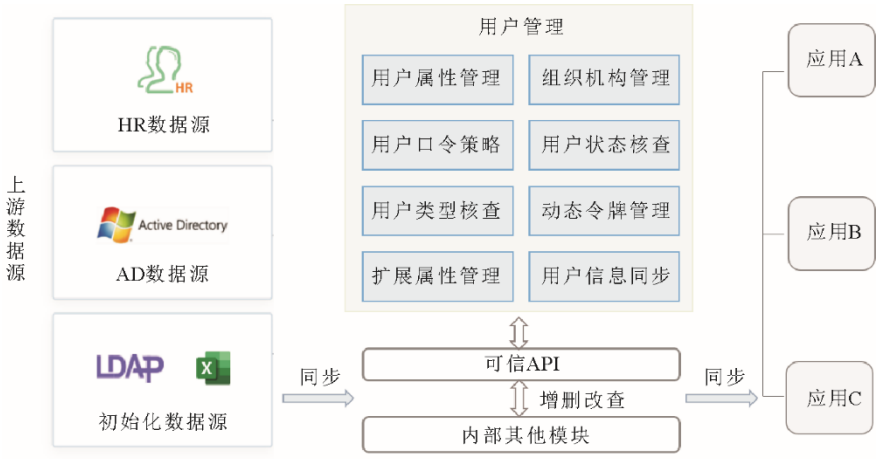


图 3 用户管理模块示意

Fig.3 Schematic diagram the user management module

授权管理包括用户的权限设置，涉及用户拥有哪些应用访问权限、用户应用账号具备哪些权限。传统方法是由管理员给用户开通应用账号并分配权限，开通账号即代表用户拥有该应用访问权限，但这种做法完全依靠人工，存在严重安全隐患以及较大管理工作量。另外，应用独立维护权限、权限与业务耦合、权限不断变化，也会导致第三方平台很难完全接管应用账号权限。因此，AAA 系统支持用户应用账号权限可在应用账号同步时授予默认权限，特殊用户账号权限由应用管理员人工调整。

零信任架构的核心思想在于，遵循“以人为核心的业务安全”核心理念，来解决企业全生命周期业务安全问题，通过对所有业务场景和资源的每一个访问请求进行强制身份鉴别和授权判定，实现按需分配资源。采用零信任的方式可以确保访问主体对资源的所有业务访问都以安全的方式进行，对所有访问请求和通信提供机密性、完整性保护和源身份验证。其中，可信代理、访问控制和信任评估为零信任架构的 3 个核心组件，零信任模型下的身份认证管理如图 4 所示，本文从以下几方面进行说明。

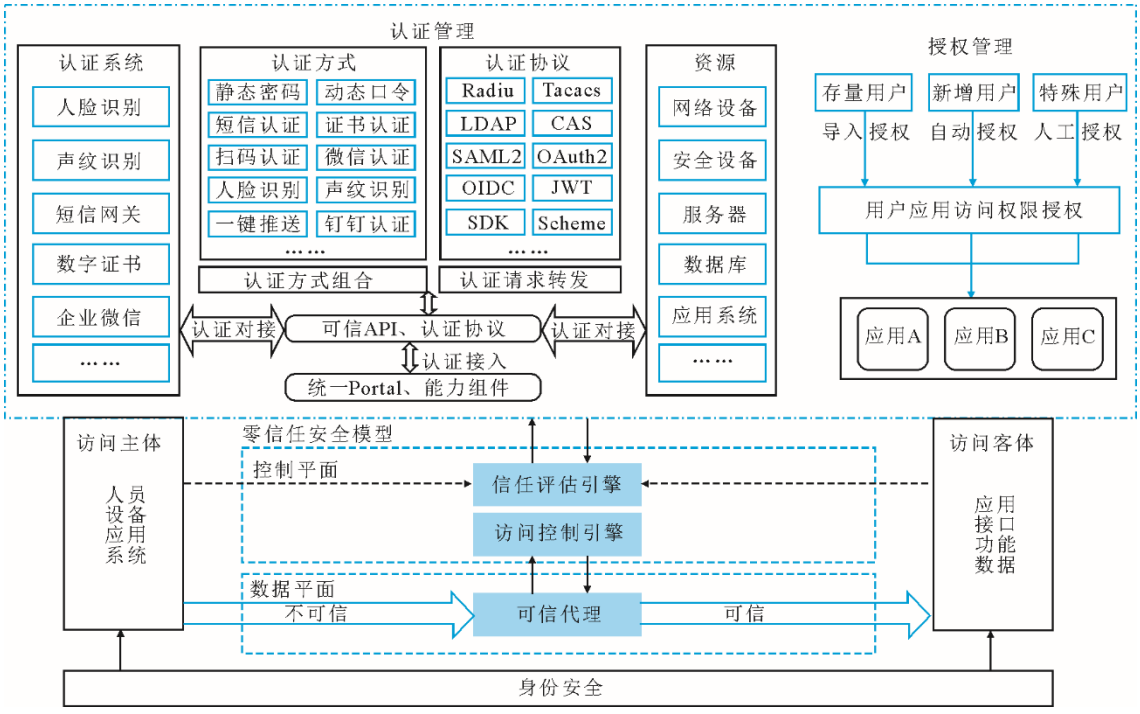


图 4 零信任模型下的身份认证管理

Fig.4 Identity authentication management under zero-trust model

1）可信代理

可信代理是确保业务安全访问的第一道关口，该组件拦截访问请求后，通过访问控制引擎可以对访问主体进行认证，对访问主体的权限进行动态判定，只有认证通过且具有访问权限的访问请求才能放行。

2）访问控制

为了确保访问主体对资源的所有业务访问都以安全的方式进行，对所有访问请求和通信都提供机密性、完整性保护和源身份验证。访问控制引擎通过结合可信代理，可以对所有访问请求进行认证和动态授权，是零信任架构控制平面的策略判定点。该组件可以对所有的访问请求进行权限判定，且不再基于简单的静态规则，而是通过上下文属性、信任等级和安全策略进行动态判定，基于实时多源数据来开展持续评估，实现动态访问控制。实时多源数据包括访问主体身份、计算环境可信度、权限策略、访问行为等，用于分析和计算的数据种类、数据可靠性有效提升持续评估准确性，同时也会考虑数据安全性、可用性、成本效率之间的平衡。

3）信任评估

信任评估引擎可对特定的网络请求或活动进行风险分析，其职责是实现持续信任评估能力，该组件可以持续接收可信代理、访问控制引擎的日志信息，再结合身份库、权限库等数据对用户身份进行持续画像，对访问行为进行持续分析，对信任进行持续评估，最终生成和维护信任库，为访问控制引擎提供决策依据，从而做到更准确的风险识别和信任评估。

1.5 审计管理

由于 AAA 系统需要对用户的身份权限与登录访问控制进行管理，因此审计功能尤为重要。传统的审计范围包括管理员操作行为、用户登录认证行为、用户访问行为。本文基于零信任架构的 AAA 系统中，审计管理模块主要是针对 AAA 系统的认证及相关操作进行日志审计，并形成统计分析，根据行为基线刻画用户行为画像，发现用户异常行为。同时支持异常行为分析管理，依托行为基线，对用户行为动作进行分析，发现登录行为异常、认证行为异常、操作行为异常、无账号异常、同一 IP 多个账号登录等，其使用场景可以分为用户登录 AAA 系统时、用户登录资源时和用户操作管理 AAA 系统时 3 种场景。

AAA 系统提供对审计事件、告警事件、用户账号管理事件和认证授权事件进行实时审计、告警和查询功能，以便管理员了解各资源和 AAA 系统自身的登录使用情况，并根据预警做出相关处理。图 5 为审计管理功能示意。

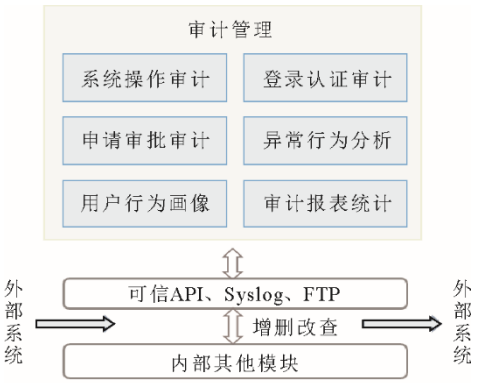


图 5 审计管理示意

Fig.5 Schematic diagram of audit management

2 AAA 系统方案设计与实现

2.1 整体功能设计

整体功能设计框架如图 6 所示。由图 6 可见，该系统包括前端、可信 API 网关、业务层、中间件和后台服务 5 个部分。前端提供平台界面，实现系统登录、用户管理、资源管理、系统管理等功能。可信 API 网关为所有请求提供路由功能。业务层包括认证中心、用户管理、资源管理、系统管理和后台服务及数据层交互，为前端提供数据支撑。中间件包括消息中心和缓存中心，实现业务层和后台服务的事件和数据交互。后台服务包括系统配置、系统日志、数据同步、账号改密等后台业务服务功能，并通过守护进程来监控 AAA 系统所有服务的运行状态[24-25]。

2.2 逻辑架构设计

AAA 系统的逻辑架构设计框架如图 7 所示。由图 7 可见，该系统逻辑架构可分为视图层、业务逻辑层和数据层。视图层提供前端展示，支持浏览器、API、PC 端、移动端等多种访问手段，并采用 SM 国密算法加密访问过程。业务逻辑层不仅实现认证、用户、系统的业务逻辑处理和控制，而且包括可信 API 网关、消息中心、缓存中心、后台服务及进程守护程序。数据层实现数据存取，认证中心、用户管理、资源管理和系统管理数据库相互独立，可以单独部署，也可以在同一个库上运行 4 个数据库实例。

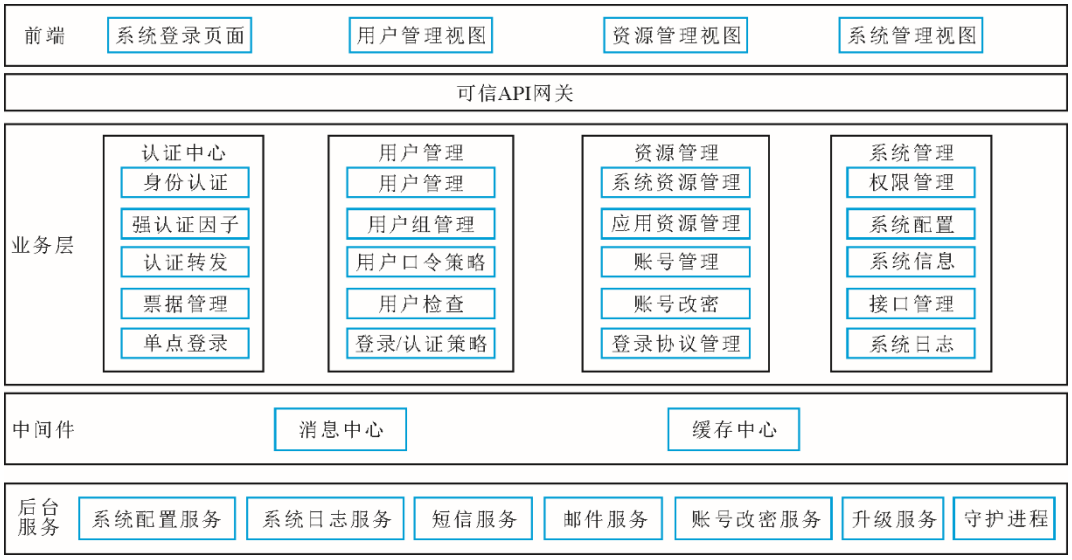


图 6 整体功能设计框架

Fig.6 Overall functional design framework

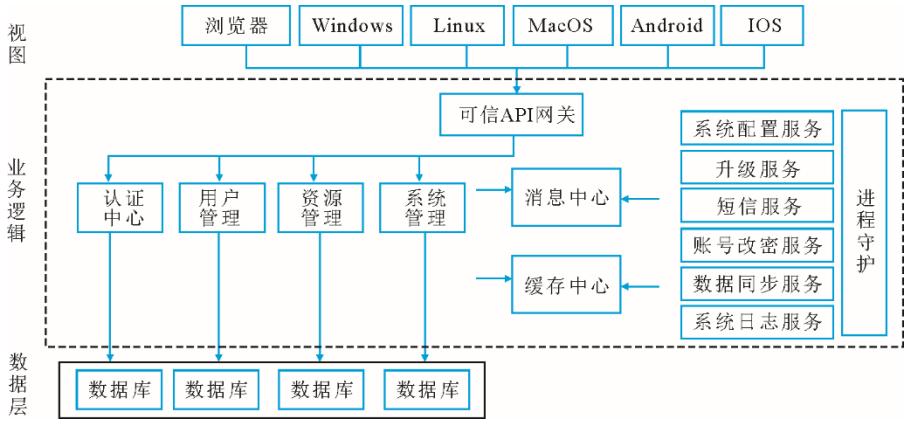


图 7 逻辑架构设计框架

Fig.7 Logic architecture design framework

2.3 零信任模块设计

身份认证管理模块是整个零信任 AAA 系统的关键部分，通过将与身份相关的数据抽离出来单独做成身份中心，结合认证中心、权限中心、应用中心、资源中心等构成整个架构体系，从而实现与各类应用在不同层级之间的对接。图 8 为身份认证管理模块整体流程。由图 8 可见，首先进行用户身份认证，通过安全接入点将认证请求转发到认证中心的处理模块，认证处理模块根据请求上下文连接到对应的身份提供商，经过一系列交互完成认证并下发访问 token。其次，用户携带相关访问 token 发起相关资源请求，在安全接入点和信任评估引擎层认证中心校验 token 的合法性以及授权、鉴权等操作，若通过校验满足访问控制策略，则提交到相关应用的 API 执行。同时，在返回数据包中还需再次校验是否满足安全策略，以及进行相应的审计日志记录。其中，信任评估引擎是由信任评估组件、大数据计算平台、智能算法等组成，根据请求上下文、信任评估模型给出实时的评估结果。

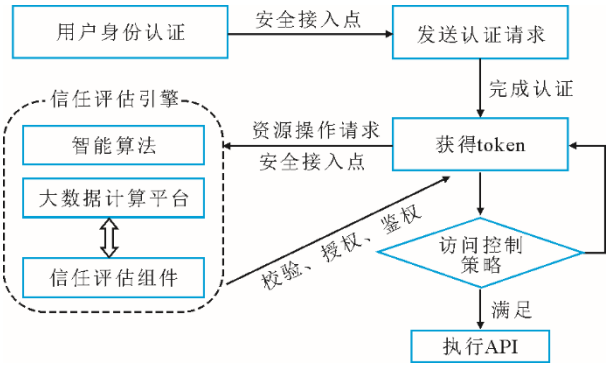


图 8 身份认证管理模块整体流程

Fig.8 Overall process of identity authentication management

2.4 AAA 子系统划分

AAA 子系统间的数据交互主要从业务数据、事件数据和缓存数据 3 个方面展开，具体描述如下。

2.4.1 业务数据

AAA 系统各服务之间通过可信 API 网关实现数据交互。可信 API 网关为所有内外部请求的入口，基于安全考虑，所有外部请求通过 https 协议请求可信 API 网关，由可信 API 网关转发请求给具体子系统，内部子系统之间的请求通过 http 协议请求 API 网关，由 API 网关转发请求给相应的子系统。可信 API 网关采用 traefik 实现。

系统管理写入系统权限和系统配置，其中系统权限管理需要读用户信息及读取资源信息。用户管理通过可信 API 网关输出用户信息，用户的权限视图需要输入系统权限。资源管理通过可信 API 网关输出资源、账号等信息，资源的协议功能需要输入系统配置。

认证中心根据用户信息、资源信息和系统配置完成身份认证，输出认证结果。数据同步需要输入系统配置信息，并把用户、资源等信息同步给各能力组件。接口服务需要输入系统配置信息，并和外部系统交互实现用户、资源等信息的双向同步。

2.4.2 事件数据

用户管理、系统管理、认证中心及数据同步、系统配置、系统升级等后台服务会产生数据变更、配置、升级、认证等事件，并把事件发送到消息中心，不同的后台服务通过订阅相应的事件完成业务操作。图 9 为具体的事件数据示意。

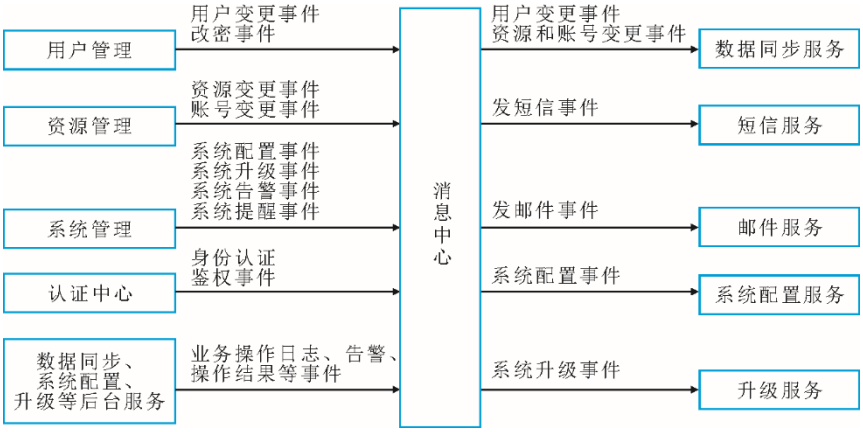
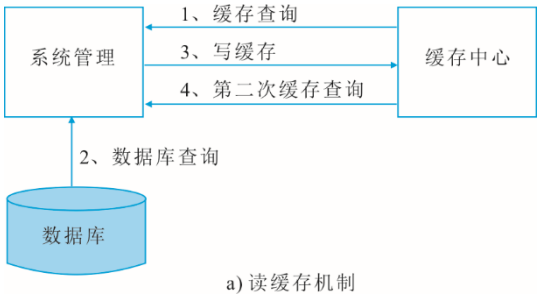


图 9 具体的事件数据示意
Fig.9 Specific event data

2.4.3 缓存数据

缓存中心把频繁读取及多个服务共用的数据缓存起来，提高数据读取的效率，减少对数据库的查询，同时多个服务可以共享缓存中心的数据，避免每个服务各自缓存数据，缓存中心遵循的原则是“使用频繁或多服务公用的数据、变更不频繁的数据”。图 10 为缓存数据处理流程，具体分为 2 步：a)读缓存机制，b)清缓存机制。



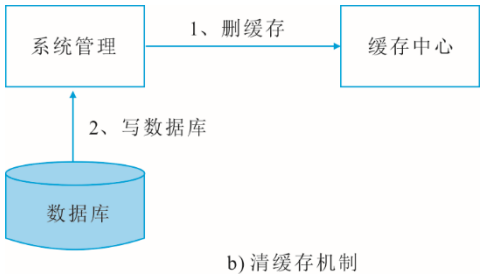


图 10 缓存数据处理流程
Fig.10 Processing flow of cache data

1）读缓存机制　以系统管理服务为例，服务查询数据时首先从缓存中读数据，第 1 次发现缓存中不存在相应数据，则从数据库查询，并把查询到的数据写入缓存中心。第 2 次查询该数据时，缓存中心已存在该数据，可从缓存中心直接读取到数据，减少了数据库访问。

2）清缓存机制　为避免数据库和缓存中心数据不一致的问题，当数据库数据需要变更或删除时，先删除缓存中的数据，再执行数据库操作。当该数据被再次使用时遵循读缓存机制，先从数据库查询最新的数据，并把查询到的数据写入缓存，供后续使用。

2.5 环境配置及性能指标

本文使用 JAVA Spring Boot 微服务架构作为 AAA 系统的开发框架，前端采用 Vue 语言，相关环境设备及软件配置见表 1，系统性能指标见表 2。

表 1 环境配置说明
Tab.1 Environmental configuration instructions

设备名称	版本
操作系统	Centos 7.7 标准版
CPU	ARM 4 核 16G
JDK	1.8.0
Eclipse	2021.9
Maven	3.8.1
Tomcat	9.0.46
Redis	5.0.14
Mysql	5.7

表 2 系统性能指标
Tab.2 System performance indicators

参数	指标
页面响应时间	AVG≤3 s，MAX≤5 s
全网账号数据同步阈值	账号同步≤1 min
并发访问（单点设备）	≥1 000
系统可靠性	双机热备持续稳定运行
系统可用率	≥99.9%
服务器 CPU 负荷率	AVG≤30%，MAX≤60%

2.6 集团级 AAA 系统部署

集团级企业的组织体系庞大，涵盖的组织结构层次复杂、数量众多，具体可划分为集团、二级单位、三级单位等，不同层级均需部署适用于当前业务需要的应用系统和设备，本文所提 AAA 系统将部署在集团总部和下辖二、三级单位，其他多级单位可以根据实际需求逐步进行细化，AAA 系统集团部署如图 11 所示。

采用多级认证场景，对于集团用户、二级单位、三级单位、本地用户，在本地完成认证；集团用户到二级单位，由二级单位先在本地查询，本地未有，由二级单位转发认证请求到集团，由集团完成认证；二级单位用户到三级单位，由三级单位用户转发认证请求到二级单位，由二级单位完成认证。

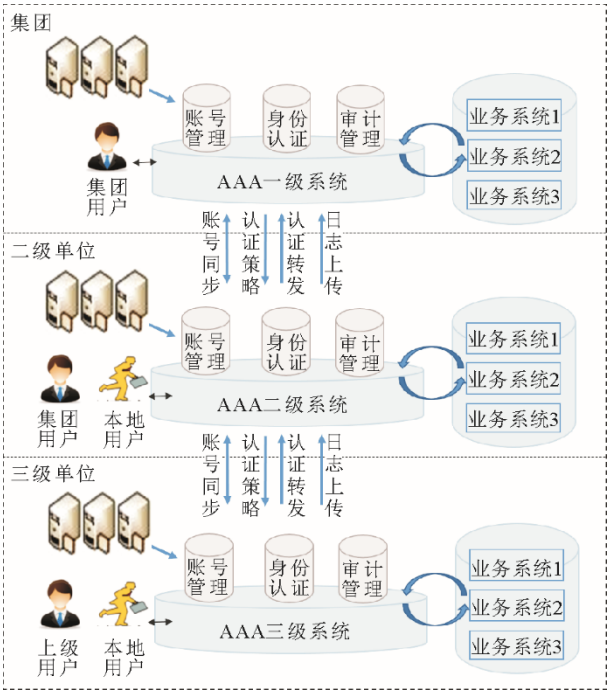


图 11 AAA 系统集团部署示意
Fig.11 Schematic diagram of group-level deployment of the AAA system

2.7 平台界面

图 12 为 AAA 系统平台入口界面，图 13—图 16 分别为用户管理、身份认证、认证方式和审计管理的部分展示界面。

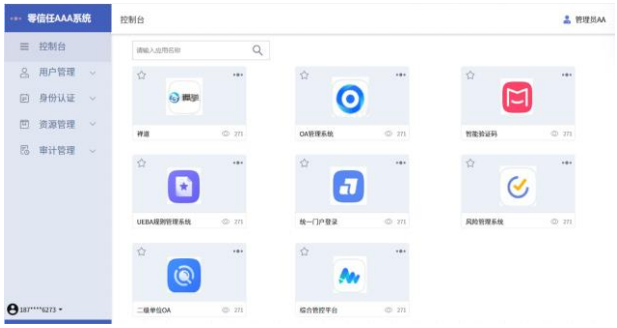


图 12 AAA 系统平台入口界面
Fig.12 Entrance interface of the AAA system platform

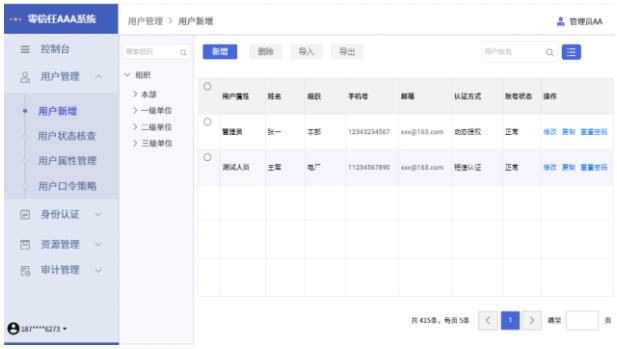


图 13 用户管理界面
Fig.13 User management interface

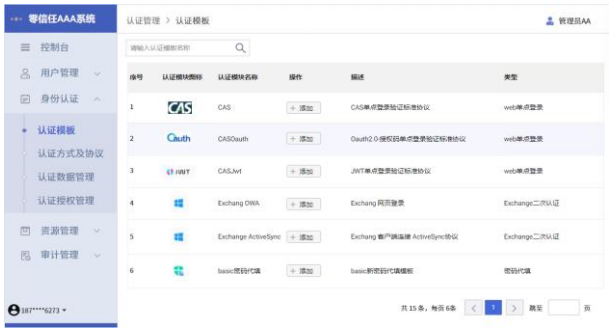


图 14 身份认证管理界面

Fig.14 Identity authentication management interface

图 15 认证方式管理界面

Fig.15 Authentication method management interface

图 16 审计管理界面

Fig.16 Audit management interface

3 结　语

为了解决目前企业信息系统中用户账号管理与安全防护的问题，实现应用系统与其他资源的统一认证和统一管理，本文提出了一种基于零信任架构的集账号、认证和审计于一体的 AAA 系统，主要定位于解决集团级企业用户账号、身份认证、用户审计管理等方面的问题。

AAA 系统的核心是关注资源统一认证和多种认证方式组合，实现用户、认证、资源和账号等配置数据的集中统一管理，并通过数据同步组件实现与外部系统数据同步。

该系统支持全面的标准协议，具备集团级全网集中的账号管理能力，能对全网账号进行集中化、标准化、可视化管理；具备集团级全网统一的认证能力，能对全网人员和业务认证提供标准化、服务化管理；具备集团级全网统一的审计能力，实现真正的有效审计。

该系统有助于提高集团级企业信息系统的业务安全，弥补了零信任环境下用户登录账号的安全问题，也进一步提高了集团级企业内网络设备、应用设备、系统和应用管理的安全防护能力。

［参 考 文 献］

［1］ 方铁城，申彦龙. 北京燃气集团统一身份认证管理平台建设与实践[J]. 城市燃气, 2020(5): 39-44.
FANG Tiecheng, SHEN Yanlong. The construction and practice of unified identity authentication management platform of Beijing gas group[J]. Urban Gas, 2020(5): 39-44.

［2］ 王静. 统一身份认证和用户管理平台在集团型电力企业的应用[J]. 信息网络安全, 2016(12): 81-85.
WANG Jing. Application of the unified identity authentication and user management platform in electric group enterprise[J]. Netinfo Security, 2016(12): 81-85.

［3］ 高鹏，陈智雨，闫龙川，等. 面向零信任环境的新一代电力数据安全防护技术[J]. 电力信息与通信技术, 2021, 19(2): 7-14.
GAO Peng, CHEN Zhiyu, YAN Longchuan, et al. A new generation of power data security protection technology for zero-trust environment[J]. Power Information and Communication Technology, 2021, 19(2): 7-14.

［4］ 李欢欢，徐小云，王红蕾. 基于零信任的网络安全模型架构与应用研究[J]. 科技资讯, 2021, 19(17): 7-9.
LI Huanhuan, XU Xiaoyun, WANG Honglei. Research on architecture and application of network security model based on zero trust[J]. Science and Technology Information, 2021, 19(17): 7-9.

［5］ 王刚，张英涛，杨正权. 基于零信任打造封闭访问空间[J]. 信息安全与通信保密, 2020(8): 78-86.
WANG Gang, ZHANG Yingtao, YANG Zhengquan. Building a closed access space based on zero trust[J]. Information Security and Communication Confidentiality, 2020(8): 78-86.

［6］ 李俊，柴海新. 数字身份安全治理研究[J]. 信息安全研究, 2021, 7(7): 598-605.
LI Jun, CHAI Haixin. Research on security governance of digital identity[J]. Information Security Research, 2021, 7(7): 598-605.

［7］ KINDERVAG J. Build security into your network's DNA: The zero trust network architecture[J]. Forrester Research, 2010, 5: 1-26.

［8］ 叶马力. 零信任安全模型在央企安全管理中的应用研究[J]. 电子世界, 2019(11): 164-165.
YE Mali. Research on the application of zero trust security model in the security management of central enterprises[J]. Electronic World, 2019(11): 164-165.

［9］ VANICKIS R, JACOB P, DEHGHANZADEH S, et al. Access control policy enforcement for zero-trust-networking[C]//2018 29th Irish Signals and Systems Conference (ISSC). Belfast: IEEE Press, 2018: 1-6.

[10] 王军峰. 零信任架构构建安全网络环境[J]. 网络安全和信息化, 2020(5): 118-121.
WANG Junfeng. Building a secure network environment with zero trust architecture[J] Network Security and Informatization, 2020(5): 118-121.
[11] 王斯梁, 冯暄, 蔡友保, 等. 零信任安全模型解析及应用研究[J]. 信息安全研究, 2020, 6(11): 966-971.
WANG Siliang, FENG Xuan, CAI Youbao, et al. Application research of zero trust architecture[J]. Information Security Research, 2020, 6(11): 966-971.
[12] 刘增明, 崔雪璐, 马靖, 等. 基于零信任框架的能源互联网安全防护架构设计[J]. 电力信息与通信技术, 2020, 18(3): 15-20.
LIU Zengming, CUI Xuelu, MA Jing, et al. Design of security framework for energy interconnection based on zero trust[J]. Electric Power Information and Communication Technology, 2020, 18(3): 15-20.
[13] WARD R, BEYER B. Beyondcorp: a new approach to enterprise security[J]. The Magazine of Usenix & Sage, 2014, 39(6): 6-11.
[14] OLTSIK J. Learning about SDP via Google Beyond Corp[Z/OL]. (2016-04-11) [2022-05-10]. https://www.csoonline. com/article/3053561/learning-about-sdp-via-google-beyondcorp.html.
[15] 左英男. 零信任架构: 网络安全新范式[J]. 金融电子化, 2018(11): 50-51.
ZUO Yingnan. Zero trust architecture: a new paradigm of network security[J]. Electronic Finance, 2018(11): 50-51.
[16] 靳起朝, 任超. 基于零信任架构的边缘计算接入安全体系研究[J]. 网络安全技术与应用, 2018(12): 26-27.
JIN Qichao, REN Chao. Research on edge computing access security system based on zero trust architecture[J] Network Security Technology and Application, 2018(12): 26-27.
[17] 万振楠. 边云一体化环境下的身份认证平台设计与实现[D]. 北京: 北京交通大学, 2020: 10.
WAN Zhennan. Design and implementation of identity authentication platform in edge cloud integrated environment[D]. Beijing: Beijing Jiaotong University, 2020: 10.
[18] 李崇智. 基于零信任架构的统一身份认证平台应用研究[J]. 信息安全研究, 2021, 7(12): 1127-1134.
LI Chongzhi. Application research of unified identity authentication platform based on zero trust architecture[J]. Information Security Research, 2021, 7(12): 1127-1134.
[19] 丁新宇. 银行金融业中生物识别身份认证技术的应用[J]. 中国新通信, 2020, 22(3): 111.
DING Xinyu. Application of biometric authentication technology in banking and financial industry[J]. China New Communications, 2020, 22(3): 111.
[20] 吕波. 以零信任技术为指导的数据安全体系研究[J]. 现代信息科技, 2020, 4(12): 126-130.
LYU Bo. Research on data security system guided by zero trust technology[J]. Modern Information Technology, 2020, 4(12): 126-130.
[21] 杨朋, 殷旻昊. SSL VPN 技术在统一身份认证平台的实现与研究[J]. 网络空间安全, 2020, 11(7): 67-70.
YANG Peng, YIN Minhao. Implementation and research of SSL VPN technology in unified identity authentication platform[J]. Cyberspace Security, 2020, 11(7): 67-70.
[22] 罗云. 简谈基于 PKI 体系的统一身份认证技术设计与实现[J]. 云南科技管理, 2021, 34(5): 62-64.
LUO Yun. On the design and implementation of unified identity authentication technology based on PKI system[J]. Yunnan Science and Technology Management, 2021, 34(5): 62-64.
[23] 王真, 马兆丰, 罗守山. 基于身份的移动互联网高效认证密钥协商协议[J]. 通信学报, 2017, 38(8): 19-27.
WANG Zhen, MA Zhaofeng, LUO Shoushan. Identity-based efficient authentication and key agreement protocol for mobile Internet[J]. Journal on Communications, 2017, 38(8): 19-27.
[24] 丁浩. 基于 MVC 模式的购物网站设计研究与实现[J]. 电脑知识与技术, 2019, 15(33): 27-29.
DING Hao. Research and implementation of shopping website design based on MVC mode[J]. Computer Knowledge and Technology, 2019, 15(33): 27-29.
[25] LIU R, WANG X. Photon-based CA authentication method and system: EP3370383A1[P]. 2018-09-05 [2022-04-05].

（责任编辑 杜亚勤）