Neusoft东软

东软统一身份管控系统

技术白皮书

目 录

1 背景

1.1 概述

随着信息业务的发展，各种信息系统的种类和数量不断增加，给信息安全管理带来了新的问题，主要包括：

1) 各应用系统相对独立且网元数量众多，无法进行统一的用户鉴权和日志管理。
2) 用户管理难度大，系统多、人员变更频繁，单纯依靠人工的方式难以实现及时有效的用户管理，大量的用户名和密码不便于维护人员记忆。
3) 各系统的日志相互独立，缺乏集中统一的系统访问审计，无法进行综合分析。

1.2 适用场景

统一身份管控系统，适合应用于各行业各领域业务系统的帐号管理、统一认证授权、综合审计运维工作中，实现对系统帐号和应用帐号集中管理和综合审计。

2 产品概述

2.1 产品简介

统一身份管控系统实现用户操作实名制，将自然人帐号与各系统上的帐号建立对应管理，实现自然人帐号与各种业务操作的对应。

统一认证支持多种认证方式。

统一授权管理实现自然人帐号与被维护资源帐号的映射关系，实现在自然人帐号对应资源帐号的一对多关系，在自然人完成认证之后能在统一身份管控系统上显示对应可访问资源的列表。

综合审计实现对多种审计部件审计数据的采集，在采集数据后进行基于访问行为的关联分析。

3 产品功能

3.1 综述

统一身份管控系统，对所管管理资源的系统帐号和应用帐号进行集中管理、统一认证、集中授权和综合审计。统一身份管控系统通过对自然人身份以及资源、从帐号的集中管理建立“自然人帐号——资源——从帐号”对应关系，实现自然人帐号与从帐号的映射关系，实现自然人对资源的统一授权，同时，对授权人员的业务操作行为进行记录、分析、展现。

3.2 集中帐号管理

集中帐号管理包含对所有服务器、网络设备帐号的集中管理。帐号和资源的集中管理是集中授权、认证和审计的基础。集中帐号管理可以完成对帐号整个生命周期的监控和管理，而且还降低了管理大量用户帐号的难度和工作量。

通过集中帐号管理，企业可以实现将帐号与具体的自然人相关联。通过这种关联，可以实现多级的用户管理和细粒度的用户授权。而且，还可以实现针对自然人的行为审计，以满足审计的需要。

3.2.1 帐号的收集与同步

统一身份管控系统能够自动发现主机、网络设备、数据库上的已有帐号。系统可以定期手动触发或自动搜索所有被管理的系统，收集所有新创建、被修改的帐号，还可以收集所有帐号与统一身份管控系统的帐号做比对。系统还可以通过帐号推送机制，通过统一身份管控系统在被管系统中创建新的帐号。

统一身份管控系统还可以与应用系统做帐号的同步。

3.2.2 帐号生命周期管理

帐号生命周期管理是指对用户从产生到删除各存在状态进行管理。包括统一的用户创建、维护、删除等功能。统一的帐号审批管理流程(添加、修改、禁用、启用、删除)。制定人员兼职、调动、离职的管理机制。

3.2.3 密码策略管理

实现集中的密码管理，并按照密码策略的要求，手动、自动、集中、定期修改系统帐号的口令，对口令强度和周期实行统一的管理。

3.3 统一认证管理

统一认证包括：自然人使用统一身份管控系统时使用的身份认证；在完成自然人认证后，选择需要访问的资源时资源帐号的认证。

3.3.1 自然人统一身份认证

为了解决传统静态口令认证存在的各种弊病和安全隐患，强认证系统采用了多因素身份认证方式来加强用户对各种系统访问前的身份认证问题。通过这些多种因素的组合，确保用户登陆时就是其本人，而不是因非法用户盗取得到的口令而登陆系统。

在统一身份管控系统中，可采用的认证方式包括：

基于同步方式的动态口令；

基于异步方式的动态口令（挑战-应答）；

数字证书；

USB口令牌；

短信认证；

生物识别技术等

通过在一个平台上支持多种身份认证手段，来实现对用户统一的身份认证和统一的身份管理。

3.3.2 资源帐号统一认证

- 网络设备的认证

在路由器、中心交换机、防火墙等网络设备中配置使用 Radius 验证，将 Radius 服务器指向到强认证服务器内置的 Radius Server。从而为网络设备的访问提供身份认证和授权。

➢ 主机系统的认证

针对 UNIX 主机操作系统，主要通过 PAM 模块或 shell 转发的方式，使用帐号管理系统自身的 Radius Server，完成身份认证；

对 Windows 系统，需要改造 GINA，完成系统的认证。

➢ 数据库系统的认证

在需要保护的 ORACLE 数据库中配置使用 Radius 验证，将 Radius 服务器指向到 SPA 内置的 Radius Server，从而为数据库的访问提供身份验证。

集中身份认证提供静态密码、Windows NT 域、Windows Kerberos、双因素、一次性口令和生物特征等多种认证方式，而且系统具有灵活的定制接口，可以方便的与第三方认证服务器对接。

3.3.3 单点登录

统一身份管控系统提供了基于 B/S 的单点登录系统，用户通过一次登录后，就可以无需认证的访问被授权的多种基于 B/S 和 C/S 的应用和系统。单点登录系统为具有多系统帐号的用户提供了方便快捷的访问途径，用户无需记忆多个系统的用户名和密码。由于单点登录系统自身是采用强认证的系统，从而提高了用户认证环节的安全性。

集中不同(B/S 架构和 C/S 架构)业务应用系统(如 ERP 等)，主机系统(如 UNIX，LINUX，WINDOWS 等)，网络设备(如交换机，防火墙)的用户身份认证。

3.3.4 外部认证

统一身份管控系统目前已经支持双因素等外部认证方式，而且系统具有灵活的定制接口，可以方便的与其它第三方认证服务器之间的结合。

3.3.5 认证策略

统一身份管控系统提供认证黑白名单策略。

3.4 统一授权管理

统一身份管控系统提供统一的界面，对用户、角色及行为和资源进行授权，

以达到对权限的细粒度控制，最大限度保护用户资源的安全。通过集中访问授权和访问控制可以对用户通过 B/S、C/S 对服务器主机、网络设备的访问进行审计和阻断。

3.4.1 集中授权

管理员在统一身份管控系统上，可以对各自的管理对象进行授权，而不需要进入每一个被管理对象才能授权。授权的对象包括用户、用户角色、资源和用户行为。系统不但能够授权用户可以通过什么角色访问资源这样基于应用边界的粗粒度授权，对某些应用还可以限制用户的操作，以及在什么时间进行操作等的细粒度授权。

3.4.2 访问控制

统一身份管控系统通过访问授权控制相应用户 B/S 访问请求，并且根据访问控制策略进行阻断、告警。

对某些 C/S 访问，可以通过堡垒主机对用户行为进行细粒度访问控制，例如 telnet、ftp、ssh 和 RDP 等。

3.4.3 堡垒主机

统一身份管控系统通过堡垒主机的形式，可以集中响应用户的各种 C/S 访问请求，包括 SSH、RDP 等远程加密访问请求，并且根据授权及访问控制策略对用户行为进行阻断、告警。

3.4.4 用户授权

通过对用户授权，可以定义用户可以访问哪些应用，以及以什么样的方式在什么时间访问。

3.4.5 角色授权

通过对角色授权，可以用户以什么身份访问应用，以及可以执行的操作。

3.4.6 资源授权

通过对资源授权，可以防止未被授权的用户、角色对资源的访问。

3.4.7 行为授权

通过制定行为授权，可以防止用户或角色对资源执行高危险的操作。例如防止用户删除重要主机上的文件、数据等。

3.5 综合审计

集中日志采集部件通过监测及采集信息系统中的系统安全事件、用户访问行为、系统运行日志、系统运行状态等各类信息，经过规范化、过滤、归并和告警分析等处理后，以统一格式的日志形式进行集中存储和管理，同时保留原始的日志信息和日志格式，以便事后分析取证用，结合丰富的日志分析综合显示功能，实现对信息系统整体安全状况的全面管理。集中日志采集部件由日志采集、日志分析、日志查询、告警查询、统计报表、设备管理和日志过滤七部分功能组成。

3.5.1 日志采集

系统采集的数据来源于网络系统中已经部署的已有的网络安全系统、主机系统和网络系统。如，防火墙/UTM、入侵检测系统、防病毒系统、网络审计系统、漏洞扫描系统、网络交换机、路由器、主机/服务器、数据库和应用服务器等。

SYSLOG 和 SNMP 协议是大多数设备支持的数据传输协议，该系统支持接收所有符合 SYSLOG 和 SNMP 协议标准的日志信息，并采用特定算法进行范式化化和存储分析。系统支持 XML、ODBC/JDBC 以及通用代理多种日志采集方式。

3.5.2 关联分析

系统将收集来的数据统一存储，支持海量数据存储，同时也支持磁盘柜、NAS 和 SAN 等多种存储方式，便于扩充和统一查询检索。

- 支持海量数据的存储；
- 系统讲采集的审计数据统一标准化，根据制定的审计策略进行关联分析，并能存储其原始日志及原始格式；

可以对安全产品、网络产品、应用系统、操作系统等产品和系统的日志信息统一进行收集、范式化并集中存储。

3.5.3 统计报表

统一身份管控系统提供的主要报表包括：

- 资源授权与访问类审计报表
- 主机与数据库类审计报表
- 业务类审计报表
- 帐号核查类审计报表

系统支持多种查询条件、以多种格式导出、统计数据汇集报表与图表。

3.5.4 审计回放

过程回放是指系统可以从审计数据库中调用一个或多个 FTP/Telnet 通信的原始数据，在显示控制台中重新显示当时的操作过程和服务器响应情况。这个功能尤其适用于对安全问题出现的原因进行事后分析和定位。

回放行为包括 FTP、Telnet、SSH，对数据库的访问行为的回放，包括 Oracle、DB2、SqlServer、sybase 等。

3.5.5 告警管理

平台支持根据预先制定的告警策略对审计事件进行分析，产生审计事件告警

并显示在平台界面，可查看告警的详细信息。

对于审计事件的告警方式，可采用平台界面显示、Email、Syslog 方式、工单、短信等。

4 产品特点

4.1 业务访问全过程审计

统一身份管控系统对业务系统中部署的认证部件、帐号管理部件、统一访问控制部件、审计部件进行集中管理，每种部件都有日志记录功能，包括认证日志、登陆日志、授权日志，而将这些日志和网络审计引擎日志进行关联，能够关联出一次整个访问过程，能够还原用户的实际操作过程。

4.2 强大的审计功能

- 精确记录用户操作时间。
- 审计结果支持多种展现方式，让操作得以完整还原。
- 审计结果可以录像回放，支持调节播放速度，并且回放过程中支持前后拖拽，方便快速定位问题操作。
- 方便的审计查询功能，能够一次查询多条指令。

4.3 安全的数据存储机制

统一身份管控系统针对管理的数据等级不同，其数据存储也是不同的。

对于帐号数据、认证数据、授权数据，采用 HA 方式实现数据库 7*24 小时不间断运行，实时提供业务支撑服务，对于所有该类数据的访问，都进行审计。

对于审计类数据，采用专用的审计数据存储设备。

4.4 可扩展性

统一身份管控系统采用模块化的开发模式，系统各模块之间可以灵活的组合与对接，而且可以通过通用接口与第三方的产品进行对接。

- 系统提供支持现有主流的各种主机设备、操作系统和应用系统；

- 系统能够提供快捷的开发平台，方便用户针对一些特有系统的二次开发；
- 硬件系统采用模块化结构，以保证系统内存、CPU 及储存容量的扩展；
- 在平台开发中保持高聚合低耦合原则，复用率高，减少系统扩展的复杂性。

4.5 高成熟性和安全性

统一身份管控系统的开发研制中，我们采用成熟的先进技术，对系统的关键技术在前期的工作中进行了大量实验和攻关及原型建立，在已开发并经广泛测试的产品中，上述的关键技术问题已解决。而且，统一身份管控系统所选取的硬件平台和软件平台，是具有良好的技术支持和发展前途的成熟产品。

系统运用了先进的加密、过滤、备份、数字签名与身份认证、权限管理等安全手段，建立健全的系统安全机制，保证了用户的合法性和数据不被非法盗取，从而保证产品的安全性。