基于大数据的自动化运维安全管控平台在电网企业的应用研究

余 萱,苏 杨,赵威扬
(贵州电网有限责任公司信息中心,贵州 贵阳 550002)

摘 要:为有效保护企业机密,保障企业数据信息安全,需要采用安全且高效的管理系统来控制企业机房运维过程中产生的信息安全风险。该文参考电网企业安全防护标准以及其它行业的安全防护设计思路,结合电网企业的业务安全防护需求以及智能化管理需要,设计了拥有智能化行为审计、自动化基线检查、自动化帐号管理、高危操作监管、动态权限分配等功能的自动化运维安全管控平台,平台以大数据分析技术为基础,通过采用模块化设计,引入大数据分析、机器学习、工作流引擎等技术,在节约管理成本和保障信息安全的同时,实现对企业信息机房运维的智能化管理。同时结合该系统在贵州电网有限责任公司信息中心的使用情况,阐述了该系统在电力企业实际环境中的应用效果。

关键词:大数据分析;统一帐号管理;自动化
文章编号:2096 - 4633(2018)12 - 0020 - 06 **中图分类号**:C39 **文献标志码**:B

1 现状与问题

随着信息化应用的迅速发展,贵州电网公司内部的各种业务和经营支撑系统不断增加,网络规模也迅速扩大。目前,公司已经形成了由大量的服务器主机、数据库系统、网络设备、安全设备、应用系统等构成的信息系统运行环境,承载着公司各大核心业务系统。而在信息系统、应用安全防护方面,公司目前采用的是分布式多点管理模式,缺少对主机服务器、数据库、中间件、网络设备等帐号统一管理的系统,无法对帐号创建、授权、权限变更及帐号撤销或者冻结全过程进行跟踪管理;无法对僵尸帐号、幽灵帐号、弱密码帐号、恶意提权帐号、过期未改密帐号进行分析和展示,容易造成帐号密码泄漏,从而可能会对业务系统的持续、健康运行造成极大安全隐患,因此,迫切需要一种行之有效的手段进行防护[1]。

运行维护部作为电网企业信息中心一线生产部门,主要职责是对贵州电网公司各信息系统进行安全管理和风险控制。

运行维护部当前面临的管理困扰如下:

(1)运维人员有限,却要肩负着对数千台服务器和数据库进行安全管控的职责,急需通过引入更先进的技术手段来提升管理效率;

(2)日常对运维工作进行的安全管控,主要通过抽查已经部署的堡垒机上的审计日志来实现,因为缺乏目的性,所以很难发现问题;

(3)日常要对安全基线配置情况进行抽查和比对核验,耗时耗力且效果一般;

(4)在运维安全管控领域中比较重要的帐号管理部分,用户除了使用堡垒机进行密码托管外,暂无其他好的管理办法[2]。

2 解决方案

通过部署一套自动化运维安全管控平台,来帮助企业提升运维安全管理效率的同时,实现对目标系统及设备帐号的自动化管理、对管理员操作行为的智能化审计、对目标系统及设备基线配置的自动化检查。

平台部署完成后,可达到以下管理目标:

(1)实现自动化帐号管理:自动发现、识别目标系统上的异常帐号,并能通过可视化方式进行风险分析展示[3];

(2)实现智能化行为审计:完整记录管理员的操作行为,自动触发高危操作告警、并实现对管理员操作行为的智能化检索和合并分析[4];

(3)实现自动化基线检查:基于企业提供的基线检查标准,定期自动到目标设备及系统上进

行相关基线配置信息采集和比对,及时发现不合规项。

3　自动化运维安全管控平台设计

为了达到上述目标,只借助传统的堡垒机是远远不够的。堡垒机的价值在于操作留痕,而在自动化、智能化管控方面无能为力,无法顺应 IT 技术发展的潮流、满足企业在管理平台上的功能需求。

本文设计的自动化运维管控平台结合对运维管理场景的深刻理解和对大数据分析、机器学习、工作流引擎等技术的引入[5],不仅能够继承堡垒机的原始功能,还能在自动化管理和安全防护要求上进一步满足电网企业的要求,同时最大程度满足电网企业在管控平台上的功能需求。

3.1　自动化运维安全管控平台设计思路

自动化运维安全管控平台在《电力行业信息系统安全等级保护基本要求》和《电力监控系统安全防护规定》的基础上,借鉴其它行业信息中心对系统运维的安全管理规定,结合电网企业信息中心目前在系统运维管理上存在的问题,梳理出自动化运维安全管控平台的具体功能如下:

3.1.1　基本功能

(1)统一登录入口:部署了自动化运维安全管控平台后,用户所有的运维操作,都必须要先登录到自动化运维安全管控平台,再经由平台自动登录目标设备。自动化运维安全管控平台是用户运维操作的唯一入口[6]。自动化运维安全管控平台的登录认证方式支持静态认证、动态双因素认证、手机令牌认证、AD 域认证、LDAP 认证、MIX 组合认证[7-12]。

(2)资源集中管理:自动化运维安全管控平台作为运维门户,既要承担用户集中登录的职责,也要承担目标资源管理集中管理的任务,用户和资源逻辑隔离却又最终在自动化运维安全管控平台上实现交汇。自动化运维安全管控平台可以统一管理主机、网络、数据库、应用四类资源类型,支持资源的批量导入和批量修改,支持资源与业务系统的关联映射和可视化展示。

(3)快速访问设备:用户登录上自动化运维安全管控平台后,即可根据管理员预先在自动化运维安全管控平台上设置好的登录规则,选择要访问的目标资源后,一键或者批量完成自动登录。

3.1.2　高危操作监管

自动化运维安全管控平台可以针对用户的重要、高危运维操作进行有效监管。监管方式为事先预防和事中控制和事后审计。

(1)事先主动防御:用户登录上自动化运维安全管控平台后,即可根据管理员预先在自动化运维安全管控平台上设置好的登录规则,选择要访问的目标资源后,一键或者批量完成自动登录。

(2)在事先预防方面,自动化运维安全管控平台可以事先制定好权限规则,当用户执行某条或者某些指令时,自动化运维安全管控平台会在命令下达给目标设备前,给予对应反馈,具体包括:允许执行、拒绝执行、切断会话、命令复核。

(3)事中实时控制:自动化运维安全管控平台针对核心系统、设备进行运维操作时,为了防止误操作的发生,采用“金库模式”进行事中权限控制:

(4)事后分类审计:用户通过自动化运维安全管控平台到目标系统、设备上进行的所有违反权限规则的命令、用户通过自动化运维安全管控平台登录到核心及重要设备时的会话复核动作,均会在审计记录中被单独提取出来以便管理员发现用户操作意图、快速定位问题[13]。

3.1.3　动态权限分配

(1)静态权限矩阵:自动化运维安全管控平台可以业务系统为视角,以资源和帐号为经纬度,以矩阵的形式展现某个业务系统内的权限分配情况。

(2)内置工单授权:自动化运维安全管控平台内置工作流,允许用户以工单的形式做资源访问申请,并提供完善的、可定制的审批流程,工单审批通过后,用户即可获取对应的访问权限。

(3)动态联动授权:自动化运维安全管控平台属于平台化的系统,采用全 API 方式进行设计。因为电网环境中存在第三方流程管理系统(如 ITSM 系统),可以通过 API 接口将自动化运维安全管控平台、ITSM 系统联动,维持用户流程管理的习惯同时实现动态授权。

3.1.4　智能行为审计

(1)全面行为审计:自动化运维安全管控平台支持图形操作审计、命令行操作审计、数据库操作审计和文件传输操作审计。

(2)智能检索合并:自动化运维安全管控平台支持根据多种条件进行会话检索,检索的结果可以直接定位到具体的操作语句/片段,并允许管理员将关注的会话操作片段进行合并查看和以时间为轴进行操作重新排序,以便于用户精准定位故障。

(3)自动对比分析:基于内置流程管理系统或第三方流程系统对接,自动化运维安全管控平台可以在流程工单到期时,对相关操作进行自动审计,并统计操作风险。

3.1.5 自动帐号管理

(1)帐号自动收集:自动化运维安全管控平台可通过远程协议,直接登录到目标系统、设备上,搜集设备上存在的所有的系统帐号(可用于运维远程登录的帐号)。帐号搜集可以覆盖操作系统、数据库、中间件层面。

(2)帐号自动巡检:自动化运维安全管控平台可以定期自动的凭借自己保管的帐号和密码,到目标设备、系统上进行巡检性质的登录测试,针对巡检过程中发现的异常,第一时间告知管理员。

(3)自动化运维安全管控平台可针对整个业务系统,设置改密计划,无需再根据具体的设备来设置繁琐的改密策略。

(4)一次性密码申请:在特殊运维场景下(如机房应急故障处理),运维人员需要获知目标设备上某个帐号的密码,以便应急开展工作。

(5)为了保证不影响用户的应急运维,同时要确保密码安全(不会外泄),自动化运维安全管控平台支持一次性密码工单申请功能。

3.1.6 自动基线检查

(1)基线标准定义:自动化运维安全管控平台可支持针对操作系统、网络设备、数据库、中间件,进行常规的自动化基线检查。检查标准可基于现有检查模版,也可自定义。

(2)配置数据自动采集:自动化运维安全管控平台支持基线配置数据的定期自动化采集或者手动一键采集,数据采集可通过远程协议直接进行,不需要在目标系统上安装 agent。

(3)检查结果可视化展示:自动化运维安全管控平台可以对采集到的数据的自动比对分析功能,及时帮助用户发现不合规配置项,并能以机房 - 业务系统 - 设备 - 配置项的形式,逐层展示异常配置项内容及受其影响的机房、业务系统或设备的范围。

3.2 自动化运维安全管控平台架构设计

自动化运维安全管控平台的设计紧跟 IT 发展潮流,以大数据分析为基础,结合工作流引擎,机器学习等技术,设计架构如图 1。

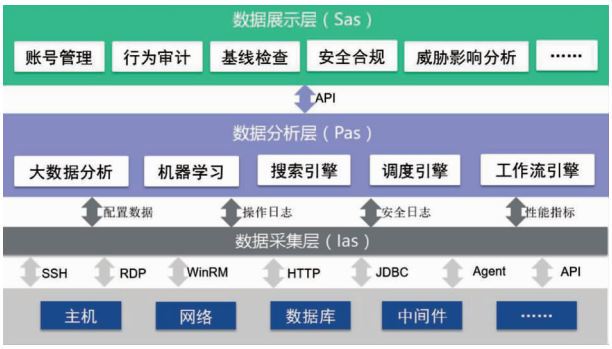

图 1 自动化运维安全管控平台架构

Fig. 1 Architecture of automatic operation and maintenance safety control platform

数据采集层:通过传统的远程协议、API,甚至 agent,自动到目标系统、设备上读取或采集各类数据[14]。而采集到的数据必经过格式化处理后,以配置数据、操作日志、安全日志、性能指标的形式,向上层提交。

数据分析层:通过内置的大数据分析、机器学习、搜索引擎、调度引擎、工作流引擎组件,对数据采集层提交的数据进行深入分析和加工,并将最终结果封装后,以 API 的形式向数据展示层交付[15]。

数据展示层:自动化运维安全管控平台最终在展示层,将数据分析层提交的数据封装成不同的功能项[16],每个功能项皆对应不同的管理场景,解决企业在不同场景下的功能需求。

3.3 自动化运维安全管控平台部署方式

3.3.1 部署方式

自动化运维安全管控平台可采用集群化部署(Active-Active-Active),来规避传统 active-standby 方式的 HA 部署带来的资源浪费、性能无法提升和服务不稳定的问题。部署逻辑示意图如图 2。

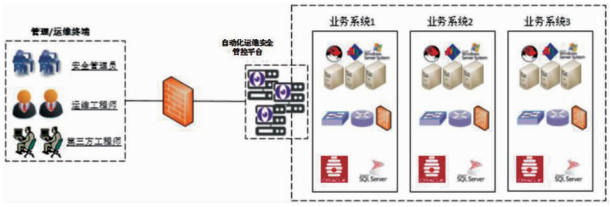

图 2 自动化运维安全管控平台部署逻辑示意

Fig. 2 Logic deployment of automation operation and maintenance safety control platform

(1)支持集群化部署,集群中设备可横向扩充;

(2)部署方式是物理旁路,逻辑串接;

(3)部署唯一条件是自动化运维安全管控平台与被管理的设备之间 IP 可达,协议可访问;

(4)在部署过程中,不需要调整任何网络架构,不需要安装任何代理程序;

(5)集中管理的一个标志就是入口唯一,自动化运维安全管控平台是管理员操作的唯一入口。

3.3.2　部署原理

如图 3 所示,每个 Node 是一个集群节点(一台安装有自动化运维安全管控平台系统的物理服务器或虚拟机),它们之间通过网络连接。

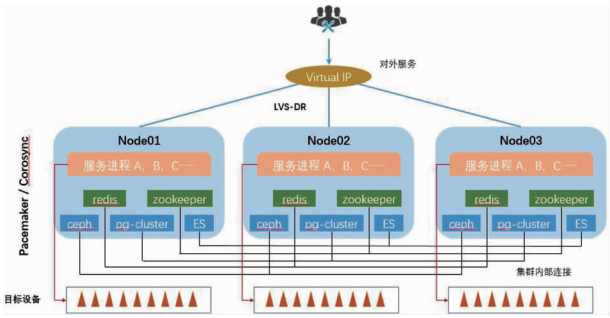

图 3　自动化运维安全管控平台网络连

Fig. 3 Automation operation and maintenance safety control platform network link

用户使用虚 IP(Virtual IP)访问自动化运维安全管控平台提供的服务(包括 Web、SSH、RDP 等)[17],集群内置调度算法,将用户的请求合理的分散到不同的节点上进行处理,以实现负载均衡[18]。

自动化运维安全管控平台功能设计思路清晰,实施部署简。

4　自动化运维安全管控平台应用成效

电网企业在应用了自动化运维安全管控平台后,实现了对现有主机、数据库系统、网络设备、安全设备、应用系统帐号的统一管理,减少了可能对业务系统的持续、健康运行的隐患发生,通过自动化手段和大数据分析,提高了安全管理的效率和安全管理的精准度。经过把数据从深度、广度、角度进行多维度聚合,让数据更加具有可读性,实现了数据的可视化。并获得了以下成效:

集中化管理是运维安全管控的前提,也是运维安全管理的必然发展趋势。通过将自动化运维安全管控平台设计成为运维门户,实现了对运维用户的集中管理,还实现了对目标资源的管理集中管理,用户和资源逻辑隔离却又最终在自动化运维安全管控平台设计实现交汇,降低了电网企业由于分布式管理造成的安全风险。

通过事先预防、事中控制、事后审计的操作行为控制措施,将由于运维过程中操作不当造成的安全事故发生率降到了最低。自动化运维安全管控平台管理员在运维过程中拥有绝对权限,可对运维人员的一切高位操作进行监控和切断。

实现了业务系统权限规则的可视化以及工单申请的流程化,自动化运维安全管控平台通过矩阵的方式展示业务系统的内的分配权限,有效的规避单纬度列表化权限展示带来的权限规则可视度差的问题。同时自动化运维安全管控平台内置工作流,允许运维人员以工单的形式申请资源访问权限。电子工单的实现,帮助企业摆托了对静态授权的依赖,解决授权不灵活、配置效率低的问题。

实现了对运维记录中的操作风险审计。自动化运维安全管控平台的智能行为审计功能会将运维人员在目标资源上的所有操作进行记录,包括图形操作、命令操作、文件传输等操作,管理员将这些行为进行智能检索合并后,实现了故障原因精准定位。

建立了一套完善的自动帐号管理体系。自动化运维安全管控平台通过帐号自动搜索、帐号自动巡检、帐号风险分析、帐号自动改密以及一次性帐号申请功能,对企业所有的设备帐号进行严谨的管理,确保企业设备帐号处于高安全性。

自动化运维安全管控平台以企业的基线检查标准,定期自动的到目标系统、设备上采集各种基线配置项,而后通过对基线配置项的比对分析,及时帮助企业发现设备异常配置。

5　结束语

随着互联网的高速发展,电力信息化已经成为电网企业发展的必然趋势,电力信息化带来的高效率、低成本、低风险使得电网企业越来越重视信息系统的建设和维护。但是电力信息化在带来巨大好处的同时,也存在一定的安全隐患[19],不管是不法份子的恶意破坏,还是企业人员在运维过程中的不当操作,都可能会给企业带来不可估量的损失。本文在《电力行业信息系统安全等级保护基本要求》和《电力监控系统安全防护规定》的

基础上,结合电网企业实际环境,设计出的自动化运维安全管控平台,实现了对企业信息系统设备帐号、系统安全配置信息、人为运维操作的全方位监控管理,将电网企业在信息化建设和系统运维过程中产生的风险降到最低。

参考文献:

[1] 成昂轩,王健弘. 一种企业信息安全风险评估模型[J]. 电脑知识与技术,2017,25:32-33,51.
CHENG Angxuan, WANG Jianhong. A model for enterprise information security risk assessment[J]. Computer Knowledge and Technology,2017,13(25):32-33,51.

[2] 王静,高昆仑,卞超轶,等. 基于大数据的能源集团统一运行监测与安全预警平台[J]. 电信科学,2018,(05):155-162.
WANG Jing, GAO Kunlun, BIAN Chaoyi, et al. Unified operation monitoring and security warning platform based on big data in energy group[J]. Telecommunications Science,2018,(05):155-162.

[3] 张云山,刘焕焕. 大数据技术在电力行业的应用研究[J]. 电信科学,2014,30(01):57-62.
ZHANG Yunshan, LIU Huanhuan. Research on application of big data technique in electricity power industry [J]. Telecommunications Sciences,2014,30(01):57-62.

[4] 王鲁平. 国家审计职业化及管理对策[J]. 审计研究,2013,(02):10-16.
WANG Luping. The professional and management measures for national audit[J]. Audit Research,2013,(02):10-16.

[5] 孙大为,张广艳,郑纬民. 大数据流式计算:关键技术及系统实例[J]. 软件学报,2014,25(04):839-862.
SUN Dawei, ZHANG Guangyan, ZHENG Weimin. Big data stream computing: technologies and instances [J]. Journal of Software, 2014,25(04):839-862.

[6] 夏明忠. 统一用户认证和授权管理的实现[J]. 计算机与应用化学,2011,28(08):1087-1090.
XIA Mingzhong. Unified user authentication and authorization of the realization of the management [J]. Computers and Applied Chemistry,2011,28(08):1087-1090.

[7] 张炳峰,徐凌宇. LDAP基本模型在数据持久层中的应用[J]. 现代电子科技,2007,30(18):140-142.
ZHANG Bingfeng, XU Lingyu. Research and application of LDAP basic model in persistence architecture [J]. Modern Electronic Technique,2007,30(18):140-142.

[8] 肖琬蓉,杨生举. 基于LDAP的统一用户认证系统设计与实现[J]. 计算机科学,2008,35(05):298-300.
XIAO Wanrong, YANG Shengju. Design and implementation of unified identity authentication system based on LDAP [J]. Computer Science,2008,35(05):298-300.

[9] 岐世峰. MIS系统中权限管理的研究和实现[J]. 电脑开发与应用,2008,21(12):8-9.
QI Shifeng. Research and implementation of authorization management in MIS system[J]. Computer Development & Applications,2008,21(12):8-9.

[10] 刘冬才. 动态身份认证系统在证券业中的解决方案[J]. 网络安全技术与应用. 2001,1(05):29-31.
LIU Dongcai. Solution of mobile identification system in stock exchange[J]. Net Security Technologies and Application. 2001,1(05):29-31.

[11] 胡立春,武友新,张烨,等. LDAP环境下的统一用户管理系统的研究与实现[J]. 计算机工程与设计. 2007,28(04):823-825.
HU Lichun, WU Youxin, ZHANG Ye, et al. Research and implementation of unified user management system in environment of LDAP[J]. Computer Engineering and Design. 2007,28(04):823-825.

[12] 唐建平. 基于LDAP技术的企业基础信息平台构建[J]. 计算机应用. 2003,23(11):66-68.
TANG Jianping. Construction of fundamental information-platform of enterprise based on the technology of LDAP [J]. Computer Applications. 2003,23(11):66-68.

[13] 梁晶亮. 上网实名制在企业的应用[J]. 贵州电力技术,2015,18(12):40-41.
LIANG Jingliang. Application of internet real name mechanism in enterprise [J]. Guihzou Electric Power Technology, 2015, 18(12):40-41.

[14] 孙大为. 大数据流式计算:应用特征和技术挑战[J]. 大数据,2015,1(03):99-105.
SUN Dawei. Big data stream computing: features and challenges [J]. Big Data,2015,1(03):99-105.

[15] 傅颖勋,罗圣美,舒继武. 安全云存储系统与关键技术综述[J]. 计算机研究与发展. 2013,50(01):136-145.
FU Yingxun, LUO Shengmei, SHU Jiwu. Survey of secure cloud storage system and key technologies [J]. Journal of Computer Research and Development,2013,50(01):136-145.

[16] 徐祗祥. 使用JSP开发Web应用系统[M]. 北京:科技技术文献出版社,2002.

[17] 郭仁超,徐玉韬. 内外网数据安全交换技术在电网企业的应用研究[J]. 电力大数据,2018,21(02):61-66.
GUO Renchao, XU Yutao. Research on the application of data security exchange technology of internal and external network in power grid enterprises[J]. Power Systems and Big Data,2018,21(02):61-66.

[18] 蒋江,张民选,廖湘科. 基于多种资源的负载均衡算法的研究[J]. 电子学报,2002,30(08):1148-1152.
JIANG Jiang, JIANG Minxuan, LIAO Xiangke. Study on load balancing algorithms based on multiple resources [J]. Acta Electronica Sinica,2002,30(08):1148-1152.

[19] 陈琪,刘涤尘,周玲. 基于Web服务的电力信息化监管系统的构建[J]. 电力系统及其自动化学报,2012,24(02):96-101.

CHEN Qi, LIU Dichen, ZHOU Ling. Construction of power information supervision system based on Web service [J]. Preceedings of the Chinese Society of Universities, 2012, 24(02): 96 – 101.

作者简介:

余　萱(1992),女,本科,助理工程师,主要从事电网信息技术研究及信息运行调度相关工作。

收稿日期:2018 – 10 – 15

(本文责任编辑:王　燕)

Research and application of automatic operation and maintenance in safety management and control platform in power grid enterprises based on big data analysis

YU Xuan, SU Yang, ZHAO Weiyang

(Information Center of Guizhou Power Grid Co., Ltd., Guiyang 550002 Guizhou, China)

Abstract: In order to effectively protect enterprise secrets and protect enterprise data information security, it is necessary to use a safe and efficient management system to control the information security risks in the process of operation and maintenance of enterprise computer room. Referring to the safety protection standards of power grid enterprises and the safety protection design ideas of other industries, combined with the business safety protection needs and intelligent management needs of power grid enterprises, this paper designs intelligent behavior auditing, automatic baseline checking, automatic account management, high – risk operation supervision, dynamic authority distribution and so on. The platform is based on the large data analysis technology. By adopting modular design and introducing the technology of large data analysis, machine learning and workflow engine, the platform can save the management cost and guarantee the information security, and realize the intelligent management of the operation and maintenance of enterprise information room. At the same time, combined with the application of the system in the information center of Guizhou Power Grid Co., Ltd., the application effect of the system in the actual environment of power enterprises is expounded.

Key words: big data analysis; unified account management; automation