徐晓庆，李新庆，黄艳红，等. 网络安全态势感知融入天镜系统的关键技术研究[J]. 中低纬山地气象，2023，47(3)：93－97.

网络安全态势感知融入天镜系统的关键技术研究

徐晓庆[1,2]，李新庆[1,2]，黄艳红[1,2]，陈增境[1,2]

（1. 中国气象局旱区特色农业气象灾害监测预警与风险管理重点实验室，宁夏　银川　750002；
2. 宁夏气象防灾减灾重点实验室，宁夏　银川　750002）

摘　要：为构建全业务、全流程、一体化、可视化的气象业务实时监控系统，提升天镜系统监控集约化能力，该文以态势感知系统融入天镜为例，从态势感知数据的确定、数据的融入、评估指标的设计、数据的可视化 4 个方面阐述了融入流程。基于 ElasticSearch、微服务和 Java 云原生可视化等关键技术，从脆弱性业务、漏洞风险态势、实时危险监控等方面设计态势感知数据在天镜中的可视化展示。

关键词：气象信息；态势感知；天镜

中图分类号：TP393.09　**文献标识码**：B

Research on Key Technologies of Network Security Situation Awareness Integration into Tianjing System

XU Xiaoqing[1,2]，LI Xinqing[1,2]，HUANG Yanhong[1,2]，CHEN Zengjing[1,2]

（1. Key Laboratory for Meteorological Disaster Monitoring and Early Warning and Risk Management of Characteristic Agriculture in Arid Regions，CMA，Yinchuan 750002，China；
2. Ningxia Key Lab of Meteorological Disaster Prevention and Reduction，Yinchuan 750002，China）

Abstract：In order to build a real－time meteorological business monitoring system with full business and full process integration and visualization，and improve the intensive monitoring capability of the Tianjing system，this paper takes the integration of situational awareness system into Tianjing as an example，expounds the integration process from four aspects：the determination of situational awareness data，the integration of data，the design of evaluation indicators，and the visualization of data. Based on the key technologies such as ElasticSearch，microservice and Java cloud native visualization，the visual display of situation awareness data in the Tianjing is designed from the aspects of vulnerability business，vulnerability risk situation，real－time risk monitoring，etc.

Key words：meteorological information；situational awareness；Tianjing

0　引言

气象综合业务实时监控系统（天镜）[1]是中国气象局统一部署的国家、省、地、县气象业务系统及数据全流程、全要素、全生命周期实时统一的监控系统，涵盖观测、预报、信息、服务各业务领域，保障了气象业务高效稳定运行。根据中国气象局集约化监控要求，2018 年和 2020 年，宁夏开展了天镜系统本地化建设，实现了气象综合业务“两横（数据全流程、业务全流程）一纵（基础设施设备）”的气象业务全流程监控信息采集、存储、加工、服务和一体化、可视化监控。

收稿日期：2022－09－01
第一作者简介：徐晓庆（1987—），女，硕士，工程师，主要从事气象信息处理工作，E－mail：519217609@qq.com。
通讯作者简介：陈增境（1984—），男，硕士，高工，主要从事气象信息网络研究，E－mail：287569721@qq.com。
资助项目：中国气象局旱区特色农业气象灾害监测预警与风险管理重点实验室科研项目（CAMP－202005）。

为应对新形势下的网络安全威胁，2022 年宁夏引进了态势感知平台，借助态势预测技术感知网络在未来一定时期内的发展情况，引导管理人员制定相应的安全策略，并对一些紧急事件进行及时预防和处理[2-3]。由于态势感知平台是一个独立的监控系统，不符合集约化监控趋势。业务人员只有登录态势感知系统提供的监控平台，才能查看网络状态信息，且平台提供的监控信息无法满足气象业务监控需求，从而导致监控运维效率低下，制约了宁夏气象业务集约化的健康发展。

本文基于省级天镜技术平台，结合关键技术，开展态势感知数据融入天镜系统的规范化研究，为气象业务系统全流程融入天镜系统，实现监控信息统一存储、统一管理和集中可视化展示提供理论指导。

1　总体设计

态势感知数据融入天镜系统的总体架构如图 1 所示，基于基础设施层，在态势感知接口规范、天镜数据接入规范和天镜应用部署规范下进行设计，由数据资源层、数据处理层、应用层构成。

（1）数据资源层是数据的访问层，以态势感知系统作为数据源。

（2）数据处理层是数据的业务逻辑层，包括两部分。①根据态势感知数据接口规范，开发数据采集模块，对态势感知中的数据进行采集。按照天镜接入标准，对采集到的态势感知数据进行标准化处理后接入天镜的 ES 数据库中。②设计符合宁夏气象信息网络安全态势的评估指标体系，从脆弱性、外部攻击、内部异常三大维度的安全实时监测能力进行构建。

（3）应用层是数据的表示层，从脆弱性、外部攻击、内部异常三大维度，开展基于天镜众创平台框架的网络安全态势感知可视化研究，对气象行业存在的信息安全问题进行可视化、多角度的展现，通过天镜 OMP 平台集中展示。

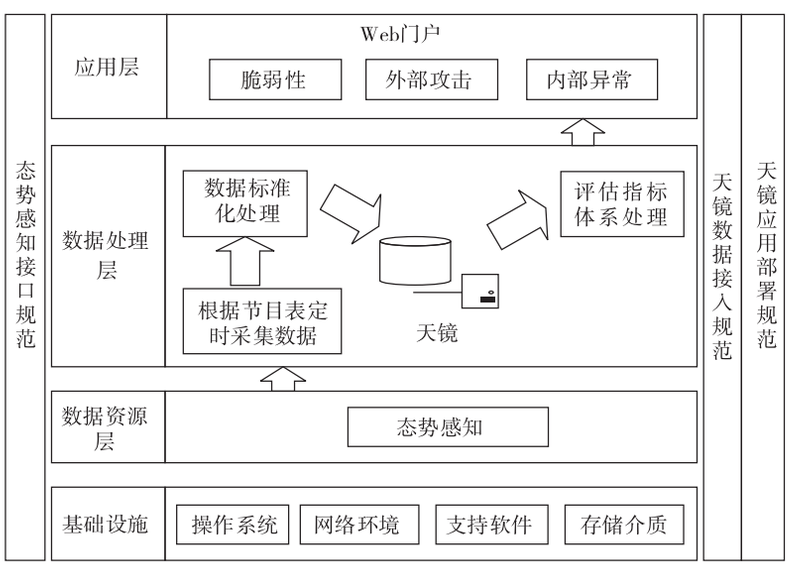

图 1　总体设计框图

Fig. 1　Overall design block diagram

2　关键技术

2.1　ElasticSearch 技术

ElasticSearch（ES）是一个分布式、高扩展、高实时的搜索与数据分析引擎，可以实时存储并检索序列化的 JSON（Javascript Object Notation）结构数据。天镜 ES 库日志根据日志类型和日期分片存储设计，索引格式如“atlantic_log_apikey_yyyymmdd”，每类日志每天生成 1 个索引，天镜 ES 数据库的 DI 和 EI 表结构如下所示。

2.1.1　DI 表结构　ES 数据库中 DI 信息字段内容如表 1，其中 type 是业务系统申请的 TYPE；occur_time 是采样时间，用 13 位时间戳表示；fields 是日志参数集合，为自定义的 JSON 串。

表 1　数据 DI 信息字段内容

Tab. 1　Content of data DI information field

序号	英文标识	属性名称
1	type	日志类型标识
2	name	日志名称
3	message	描述信息
4	occur_time	采样时间
5	fields	日志参数集合

2.1.2　EI 表结构　ES 数据库中 EI 信息字段内容如表 2,其中 type 是固定类型 SYSTEM. ALARM. EI;EVENT_TYPE 是事件类型,根据监视信息接口规范要求定义,由 6 段字符组成,格式为 AA_DDD_E - F - GG - HH(如:OP_CIPAS_A - 1 - 10 - 01);EVENT_LEVEL 是事件级别,0:恢复,1:警告,2:关键,3:严重;EVENT_TITLE 是事件标题,最大长度为 255 字节。

表 2　数据 EI 信息字段内容

Tab. 2　Content of data EI information field

序号	属性名称	英文标识
1	type	ES 类型
2	occur_time	时间戳
3	SYSTEM	业务系统名称
4	EVENT_TYPE	事件类型
5	EVENT_LEVEL	事件级别
6	EVENT_TITLE	事件标题
7	KEvent	故障内容

2.2　微服务技术

采用微服务接口技术,将态势感知平台信息接入监控系统,可有效解决监控系统与态势感知系统“紧耦合”问题[4]。监控系统与态势感知系统的数据库物理分离,性能相互不受影响。通过微服务接口抽取态势感知的 KPI 信息接入监控系统,降低了态势感知系统直接向监控系统数据库写入信息造成入库延迟、信息丢失等情况的发生率。

微服务架构模式就是将整个 Web 应用组织为一系列小的 Web 服务。这些小的 Web 服务可以独立编译和部署,并通过各自暴露的 API 接口相互通信。它们彼此相互协作,作为一个整体为用户提供功能,却可以独立地进行扩展[5]。如图 2 所示,不同的微服务通过注册中心注册,对外提供访问 API。通过负载均衡(nginx),相同的微服务实际运行于不用的服务器(SERVICR)中。客户端访问系统时,通过网关(GATEWAY)判断访问的请求,将相应的服务返回。系统内部通过 nginx 调用环境压力较小的服务器,保证服务的高可用。通过微服务 API 接口接入态势感知监控信息,易于后期维护,可根据不同的业务需求和系统更新,及时进行接口变更和调整,以满足后续气象业务发展的需求。

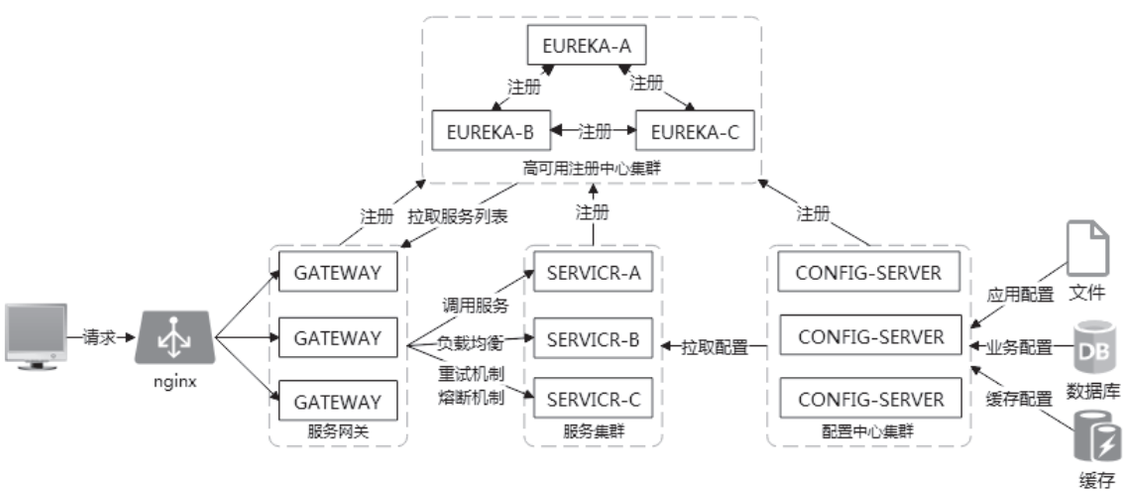

图 2　微服务 API 流程图

Fig. 2　Micro service API flowchart

2.3　Java 云原生可视化技术

基于天镜众创平台开发环境,依托接入的态势感数据,开展可视化设计。使用 RabbitMQ、Redis 等中间件搭建应用架构,实现态势感知数据的接入和处理;借助众创平台 DevCenter 模块,采用 Java 云原生代表技术 Kubernetes[6]、ServiceMesh、SpringCloud[7]等构建基础平台层;采用 SpringBoot、MyBatis 等实现本地化开发,通过 OMP 平台完成安装部署及应用,具体技术框图如 3 所示。

3　融入流程

融入流程主要包括 4 个部分,即态势感知数据确定、态势感知数据采集并入库、气象信息网络安全态势评估指标设计、态势感知数据可视化。

3.1　确定态势感知数据

根据态势感知数据接口规范,收集网络安全攻击、用户行为分析、信息数据泄露等数据的 KPI 信息,主要包括受监控 IP 模块数据、资产信息终端数

据、风险业务及终端数据、安全事件数据、脆弱性数据等[8-9]。

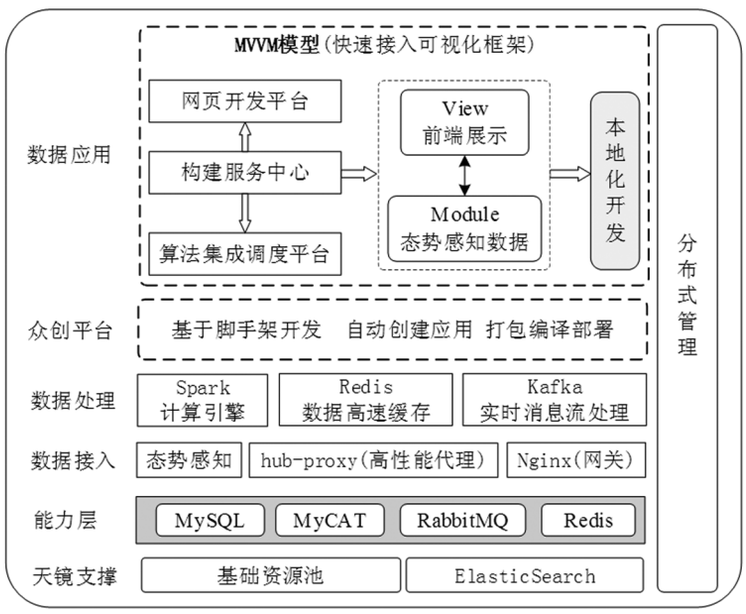

图 3　Java 云原生可视化

Fig. 3　Java cloud native visualization

态势感知数据接口规范如图 4 所示。接口使用 HTTPS 协议承载通信数据,用户调用登录接口,获取认证 token,再通过携带的 token 访问业务接口,最终获取 JSON 格式的态势感知数据。

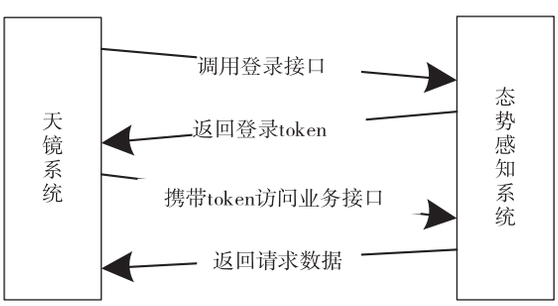

图 4　态势感知数据接口规范

Fig. 4　Situation awareness data interface specification

3.2　态势感知数据融入天镜

3.2.1　建立 TYPE　根据天镜数据接入规范,在天镜系统建立态势感知数据专属 TYPE(BEYC. NXTS. SERVICE. DI)。

3.2.2　开发采集模块　采用微服务技术设计开发采集模块,根据态势感知数据接口规范,通过定时任务定时采集态势感知接口的数据(DI 和 EI)。根据天镜 ES 数据库的存储规范,将采集到的 DI 和 EI 进行标准化处理后推送至天镜系统。天镜的采集接口为:http://IP 地址/store/openapi/v2/logs/push_batch? apikey = KEY。

3.2.3　数据入库　采集模块推送至天镜系统的 DI 和 EI,由天镜日志网关(log – gateway)处理,通过预处理模块处理后发送给 Kafka、Spark Stream 等实时并行计算框架进行数据的加工处理,日志写入模块(log – writer)将态势感知数据 DI 和 EI 写入天镜 ES 数据库的 atlantic_log_apikey_yyyymmdd 索引中[10]。

3.3　设计态势感知评估指标

宁夏气象信息网络安全态势评估指标是运行信息网络安全态势感知的基础,必须具备多维度的监测、分析体系。本文结合等级保护 2.0 三级系统基本要求,分析网络中重点关注的安全点,从脆弱性、外部攻击、内部异常三大维度的安全实时监测能力进行构建,设计气象信息网络安全态势评估指标,如表 3 所示。

表 3　安全态势评估指标体系

Tab. 3　Security situation assessment index system

一级指标	二级指标
脆弱性	漏洞
	明文传输
	弱密码
	风险端口
外部攻击	高危攻击
	暴力破解
	漏洞利用攻击
	WEBSHELL 后门植入
内部异常	失陷主机检测
	横向威胁感知
	外连威胁感知

3.4　态势感数据可视化

3.4.1　监控大屏的设计　根据态势感知评估指标,从脆弱性、外部攻击和内部异常状态三大维度展开,设计态势感知监控大屏,大屏功能模块主要包括脆弱性业务、重点资产监视、漏洞风险态势、实时危险监控、安全事件、网络攻击和威胁等级。

3.4.2　监控大屏的开发　(1)天镜众创平台开发流程。通过天镜众创平台创建应用并更新到 Git[11] 仓库,启动集成在开发环境中的本地化程序进行开发调测,调测通过后在测试环境中发布应用,进行联调测试直到测试通过,符合发布标准之后在工单系统中提交应用上线申请,待系统管理员审批通过后。通过 OMP 平台将态势感知监控大屏模块发布至生产环境。天镜众创平台开发流程如图 5 所示。

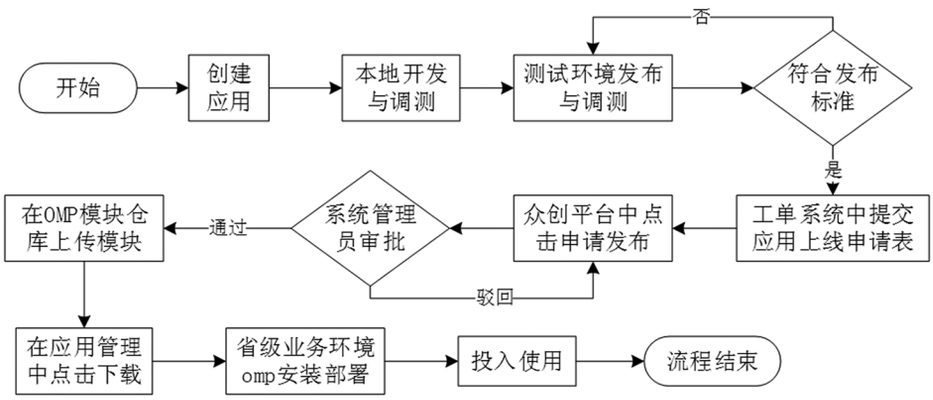

图 5　天镜众创平台开发流程

Fig. 5　Tianjing maker platform development process

(2)本地化开发。天镜众创平台开发流程中的本地化开发,是基于天镜众创平台 DevOps(Development 和 Operations)[12-13] 框架,根据天镜 ES 数据库存储规范,采用 Java 云原生中的 SpringBoot、MyBatis 和 Echarts 等技术,获取天镜 ES 数据库中的态势感知数据,根据监控大屏的设计,开发宁夏气象信息网络安全态势感知监控大屏,在天镜系统中部署、展示。

4　总结

监控集约化是未来监控的趋势,宁夏气象局作为天镜 2.0 试点省,其他业务监控信息融入天镜系统已迫在眉睫。本文以态势感知监控信息融入天镜系统作为研究突破口,阐明了融入过程中 Elastic-Search、微服务、Java 云原生可视化等关键技术,详细梳理了融入流程,为网络安全态势感知信息在天镜系统集中展示、统一管理和统一预警提供理论依据,同时,也为后续其他业务系统融入天镜系统提供参考,更好地推动宁夏气象信息化建设。

参考文献

[1] 孙超,肖文名,陈永涛,等. 气象综合业务实时监控系统的设计[J]. 气象科技进展,2018,8(1):153-157.

[2] 陈澍,孟金,冯勇,等. 态势感知技术在省级气象网络安全防护中的应用[J]. 信息技术与信息化,2020(10):127-129.

[3] 邓鑫,田征,李楠,等. 浅析网络安全态势感知技术在气象网络中的实践与应用[J]. 网络安全技术与应用,2020(5):139-140.

[4] 全力. 基于微服务架构的气象数据处理与可视化平台研究[D]. 南京:南京信息工程大学,2022.

[5] 杨天一. 论微服务架构的优势与劣势[C]//第三十六届中国(天津)2022'IT、网络、信息技术、电子、仪器仪表创新学术会议论文集,2022:294-297.

[6] 李轲,窦亮,杨静. 面向 Kubernetes 的多集群资源监控方案[J]. 计算机系统应用,2022,31(7):77-84.

[7] 付博. 基于 SpringCloud 的绿植养护软件的设计与实现[D]. 北京:北京邮电大学,2021.

[8] 王娟,张凤荔,傅翀,等. 网络态势感知中的指标体系研究[J]. 计算机应用,2007(8):1907-1909.

[9] 陈丽莎,张凤荔,王娟. 构建网络安全态势评估指标体系[J]. 重庆科技学院学报(自然科学版),2008,45(3):135-137.

[10] 袁雅涵,冯勇,朱辉,等. 基于多源数据的快速统一监控关键技术研究[J]. 电子技术与软件工程,2022(6):241-245.

[11] 徐娅. Git 版本控制工具在团队协作项目中的应用[J]. 智能计算机与应用,2019,9(5):341-343.

[12] GLAZEMAKERS Kurt. Opening the network to DevOps without letting threats inside[J]. Network Security,2021,2021(12):7-9.

[13] 张冬松,胡秀云,邬长安,等. 面向 DevOps 的政务大数据分析可视化系统[J]. 计算机技术与发展,2020,30(8):1-7.