文章编号：2096-1472(2021)-04-43-03
DOI:10.19644/j.cnki.issn2096-1472.2021.04.010

基于Prometheus的油田数据泄漏防护大数据系统运维方法

王晓锋，马丽丽

(大庆油田信息技术公司，黑龙江 大庆 163000)
✉wangxf1987@126.com; malili1220@126.com

摘　要：数据泄漏防护系统可以阻止企业的重要数据从网络出口违规外发。针对油田数据泄漏防护大数据平台对各个区域、不同类型的数据采集和设备、业务监测问题，本文首先提出依托大数据Flume(数据采集系统)组件，采用抓取外泄事件日志JSON(一种轻量级的数据交换格式)和解析后的违规外发文件txt文本的方法，实现数据采集；其次依托Prometheus服务监管系统Flume_exporter、Node_exporter组件和Grafana(一个跨平台的、开源的度量分析和可视化工具)，实现对数据泄漏防护设备信息和应用数据的监管；最后指出搭建采集系统和监管平台对数据泄漏防护系统运维的作用。

关键词：Flume；Prometheus；数据采集；监管平台
中图分类号：TP391　**文献标识码**：A

Operation and Maintenance Method of Big Data System for Oilfield Data Leakage Prevention based on Prometheus

WANG Xiaofeng, MA Lili

(*Daqing Oilfield Information Technology Company*, *Daqing* 163000, *China*)
✉wangxf1987@126.com; malili1220@126.com

Abstract: Data leakage protection system can prevent important data of enterprises from being illegally exported from networks. This paper aims to solve problems of acquiring data of different types in different regions, and monitoring equipment and business on big data system for oilfield data leakage prevention. First, based on big data Flume (data acquisition system) component, this paper proposes to adopt the method of capturing JSON (JavaScript Object Notation, a lightweight data exchange format) of the leakage event log and the parsed illegally exported TXT file to achieve data acquisition. Second, Flume_exporter (Prometheus service supervision system), Node_exporter component and Grafana (a cross-platform open source measurement analysis and visualization tool) are used to supervise equipment information and application data of data leakage prevention. Finally, this paper points out the effect of building an acquisition system and supervision platform in operation and maintenance of data leakage prevention system.

Keywords: Flume; Prometheus; data acquisition; supervision platform

1 引言(Introduction)

随着信息技术的快速发展，数据量成几何级数增长，人类进入大数据时代。在大数据分布式集群系统环境下，实现满足每秒数百MB的日志数据采集和传输需求，已经成为大数据解决方案的前提和基本保障。如何解决在复杂场景下技术实现高纬度数据模型、自定义语言查询、可视化数据展示等数据监控技术难题，也成为大数据解决方案的一项严峻的挑战[1]。

油田企业为防护重要数据资产不从网络出口违规泄漏，搭建了油田数据泄漏防护大数据系统。本文主要研究依托开源数据采集系统Flume，实现油田对网络、终端敏感文件外泄事件全面数据采集，并且基于Prometheus服务监管系统[2]搭建油田数据泄漏防护大数据监管平台，实现对数据泄漏防护设备基本信息和应用数据的实时监控、管理、分析以及健康度

准确评估。

2 Flume数据采集系统(Flume data acquisition system)

Flume是一个高可靠、分布式、高可用的海量日志采集、聚合和传输系统，将大批量不同数据源的日志数据收集、聚合、移动到HDFS进行存储[2]。Flume分布式系统的核心是Agent，内部有三个组件：Source、Channel、Sink。Source：源数据采集，通过与应用服务接口对接以获取数据；Channel：Agent内部的数据传输通道，作为临时存储聚合数据，用于从Source将数据传递到Sink；Sink：从Channel消费数据并将其传递给目标地，最终将数据存储到集中存储器(HDFS)。Flume数据采集系统架构图如图1所示。油田数据泄漏防护大数据采集系统就是对终端、网络数据泄漏防护日志、文件通过Flume Agent采集工具，以不同的Topic形式统一传输到Kafka，最终存储到HDFS中。

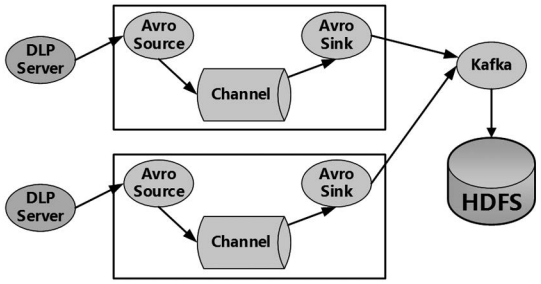

图1 Flume数据采集系统架构图

Fig.1 Architecture diagram of Flume data acquisition system

Flume在收集数据过程中，可以定义JMX、JSON、Custom等格式采集报告，并通过配置Web服务器展示，实现对传输数据的实时监控。由于Flume数据采集报告Web展示端不具备大规模数据仪表盘式展示，在大数据背景下，借助Prometheus监管平台以图表形式简洁、直观地展示并统计、分析采集数据。

3 Prometheus监管平台(Prometheus supervision platform)

Prometheus是一个开源的服务监控系统和时间序列数据库，目前已经被广泛应用于数据中心监控[3]。Prometheus可以对系统资源或指定业务资源实时监控，对自定义时间段内的数据参数进行查询、分析，实现高效的系统维护和实时健康评估。

3.1 Prometheus组件介绍

Prometheus核心组件包括Prometheus Server(服务器)、Exporter(采集主机的监控样本数据程序)、PushGateway(数据中转网关)、AlertManager(告警系统)。

Prometheus Server：负责实现对监控数据的获取、存储及查询。Prometheus Server可以通过静态配置管理监控目标，也可以配合使用Service Discovery的方式动态管理监控目标，并从这些监控目标中获取数据。Storage模块将采集的数据保存在TSDB(时序数据库)中，最终按照时间序列的方式存储在本地磁盘中。

Exporter：将监控数据采集的端点(Endpoint)通过HTTP服务的形式暴露给Prometheus Server，Prometheus Server通过访问该端点获取到需要采集的监控数据。

PushGateway：当网络环境不允许Prometheus Server和Exporter进行通信时，可以使用PushGateway来进行中转。PushGateway将监控数据主动推送到Gateway中，然后Prometheus Server从PushGateway中拉取监控数据。

AlertManager：在Prometheus Server中支持基于PromQL创建告警规则，如果满足PromQL定义的规则，则会产生一条告警。当接收到告警后，会通过邮件、钉钉等方式发出告警。

Grafana是一款美观、强大的可视化监控指标展示工具，主要用于大规模指标数据的可视化展现，是网络架构和应用分析中最流行的时序数据展示工具。它将Prometheus监控的数据源以仪表盘方式在Web面板展示。

Prometheus技术架构图如图2所示。

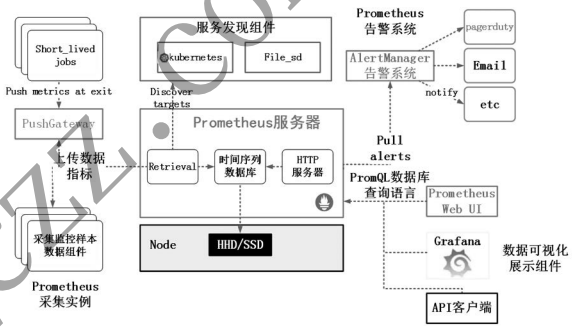

图2 Prometheus技术架构图

Fig.2 Technical architecture diagram of Prometheus

3.2 Prometheus的工作流

Prometheus Server定期从Exporter中拉取数据，或者接收来自PushGateway推送的数据；Prometheus Server在本地存储收集到的数据，并运行定义好的告警规则，记录新的时间序列或者向AlertManager推送警报；AlertManager根据配置文件对接收到的警报进行处理，发出告警；在Grafana图形界面中，可视化展示数据。

4 油田数据泄漏防护大数据采集系统和监管平台(Big data acquisition system and supervision platform for oilfield data leakage prevention)

油田数据泄漏防护大数据采集系统的目标是通过Flume 1.8.0采集油田企业违规外发敏感数据产生的外泄事件和油田企业内部终端资产信息(包括软硬件信息、终端存储文件信息、组织机构信息等)，根据不同类型Topic，统一传输到Kafka，为数据泄漏防护大数据平台提供分析、建模的数据源，采集数据最终存储到HDFS中。

油田数据泄漏防护大数据监管平台基于Prometheus监控系统Flume_exporter组件采集Flume获取数据的统计数量，Node_exporter组件获取数据泄漏防护设备系统运行状态，AlertManager组件进行异常告警，Grafana工具在Web面板展示，实现数据信息的分析和监控。油田数据泄漏防护大数据

采集系统和监管平台架构图如图3所示。

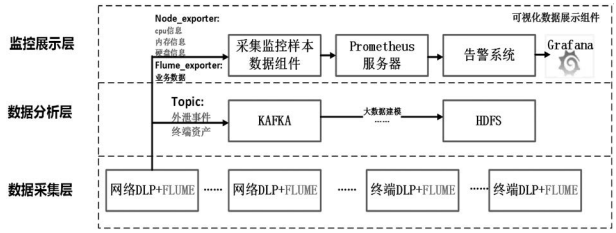

图3 油田数据泄漏防护大数据采集系统和监管平台架构图

Fig.3 Big data acquisition system and supervision platform architecture diagram of oilfield data leakage prevention

4.1 油田数据泄漏防护大数据采集系统

根据Flume Agent采集数据泄漏防护外泄事件和网络资源业务需求，进行项目定制开发，形成FileLimitrateThriftInterceptor.java，修改配置文件thrift2kafka.conf，实现将数据传输至大数据Kafka组件[4-5]。FileLimitrateThriftInterceptor.java部分代码如下：

```
public FileLimitrateThriftInterceptor(Context context)
    {
            this.context = context;
//采集数据初始化
    public void initialize() {
        //根据标记iscollect决定是否启用该通道
        this.flag=context.getBoolean(ISCOLLECT, true).
booleanValue();
        this.secretkey = context.getString(SECRETKEY);
        try {
          this.aesUtils = new AesUtils(this.secretkey);
        } catch (Exception e) {
            e.printStackTrace();
            logger.info("aesUtils initialize error");
//获取事件方法
    public Event intercept(Event event) {
        ArrayList<byte[]> bytes = new ArrayList
<byte[]>();
         bytes.add(addBytes(event.getBody()));
         if(isUseSecret){
event.setBody(aesUtils.AESEncode(SerializableUtils.
ObjectToByte(bytes)));
         }else{
         event.setBody(SerializableUtils.ObjectToByte
(bytes));
    public List<Event> intercept(List<Event> events) {
          for (Event event : events) {
             intercept(event);
```

thrift2kafka.conf配置文件如下：

```
//配置Source
a1.sources.r1.type=thrift
a1.sources.r1.port=9110
a1.sources.r1.interceptors=limitrate
a1.sources.r1.interceptors.limitrate.type=src.
interceptor.FileLimitrateThriftInterceptor$Builder
//配置Channel
a1.channels.c1.type=file
a1.channels.c1.checkpointDir=/mnt/checkpoint1
a1.channels.c1.dataDirs=/mnt/file-channel1
//配置Sink
a1.sinks.k1.type=org.apache.flume.sink.kafka.
KafkaSink
a1.sinks.k1.kafka.topic=FILE_STORE_TOPIC
a1.sinks.k1.kafka.bootstrap.servers=kafka01.dqyt.
com:9092
```

4.2 油田数据泄漏防护大数据监管平台

油田数据泄漏防护大数据监管平台建设包括三部分：Exporter组件代码编写；告警规则AlertRule配置，AlertManager组件进行异常处理方法配置；Grafana工具在Web面板展示方法配置[6-7]。

4.2.1 Exporter组件

采用Go语言开发Flume_exporter、Node_exporter组件代码，获取Flume端采集数据数量和服务器系统资源数值。Exporter部分核心代码如下：

```
go func() {
    defer wg.Done()
    for _, url := range e.flumeMetricUrls {
      m := <-channel
      if m.Metrics[url] == nil {
        log.Warn(">>>.receive metrics channel is nil,
url:" + url)
        continue
      }
      reg := regexp.MustCompile('//(.*)/metrics')
      host := reg.FindStringSubmatch(url)[1]
      for k, v := range m.Metrics[url] {
        sMetrics := make(map[string]interface{})
        sMetrics = v.(map[string]interface{})
        delete(sMetrics, "Type")
        if strings.HasPrefix(k, "SOURCE.") {
          e.processGaugeVecs(k, host, "SOURCE",
sMetrics)
        } else if strings.HasPrefix(k, "CHANNEL.") {
          delete(sMetrics, "Open")
          e.processGaugeVecs(k, host, "CHANNEL",
sMetrics)
        } else if strings.HasPrefix(k, "SINK.") {
          e.processGaugeVecs(k, host, "SINK",
sMetrics)
```

4.2.2 Grafana界面展示

Grafana平台配置页面定义与Prometheus链接的变量后，配置展示的JSON Model。配置变量Variable如下：

```
Variable:
$host  label_values(host)
$channel_name
label_values(FLUME_CHANNEL_ChannelSize{host=
"$host"},name)
$sink_name
```

label_values(FLUME_SINK_EventDrainSuccessCount{host="$host"},name)

$source_name

label_values(FLUME_SOURCE_OpenConnectionCount{host="$host"},name)

4.2.3 AlertManager告警

制定Prometheus服务器中的警报规则，规则触发时，将警报发送到AlertManager组件。告警处理方法包括沉默、抑制、聚集和通过，例如邮件、即时通讯平台、钉钉等。

4.3 测试及运行结果

Flume数据采集系统以流处理形式采集数据泄漏防护产生外泄事件JSON和解析的违规文件txt，系统性能测试需求是找出每秒接收事务数(外泄事件JSON数)峰值和Flume系统处理最大size文件需要的平均时间，生产环境要求最大文件为50 MB。测试结果为：每秒接收事务数峰值613条,处理事务数1.5 Mbps，处理50 MB大小解析文件需要30多秒。

Prometheus数据监控系统批处理形式获取数据，只需对采集数据和告警功能的接口功能进行测试。

5 结论(Conclusion)

利用大数据组件Flume的油田数据泄漏防护大数据采集系统为大数据分析展示平台提供了数据源，为油田数据泄漏防护大数据解决方案提供了数据基础。搭建Prometheus监管平台实现数据泄漏防护设备基本信息和Flume采集数据实时监控、管理、分析和健康度准确评估。在数字化油田的推动下，信息化产品类型更加多样，设备数量、复杂度逐年增加，为网络运维带来巨大的挑战。油田数据泄漏防护大数据监管平台全面监控油田数据泄漏防护大数据系统下所有运行设备，大大降低了人工运维成本和设备运行风险。

参考文献(References)

[1] 何邦才.大数据技术下企业信息采集技术研究[J].无线互联科技,2019(4):58-59.

[2] 方中纯,赵江鹏.基于Flume和HDFS的大数据采集系统的研究和实现[N].内蒙古科技大学学报,2018(9):153-155.

[3] 马永,吴跃,何李囡.基于Prometheus的基础软硬件全链路监控设计和实现[J].电子技术与软件工程,2019(24):39-40.

[4] 林苍.基于flume的日志收集统计系统[D].福建:厦门大学,2013(7):13.

[5] 张小龙.基于Flume的XML数据自动收集系统[J].科学技术与工程,2013(13):9062-9064.

[6] 陈晓宇.深入浅出Prometheus:原理、应用、源码与拓展详解[M].北京:电子工业出版社,2019:60-77.

[7] JULIUS V. Prometheus monitoring system best practices and common pitfalls[C]. QCon北京2018大会, 2019.

作者简介：

王晓锋(1989-)，男，本科，工程师.研究领域：软件研发，大数据运维.

马丽丽(1982-)，女，本科，高级工程师.研究领域：软件开发.

(上接第54页)

目标停车场；用户更无须担心车辆安全，APP实时向用户更新车辆信息和停车状态信息。软件系统的应用降低了人工成本，很好地提高了工作效率。

参考文献(References)

[1] DU B. Smart home system based on intelligent cloud Internet of Things[J]. Future Generation Computer Systems, 2018, 8(6):98-105.

[2] JIA L. Research and development of open laboratory management system based on web technology[J]. Neurocomputing, 2017, 5(4):200-215.

[3] 李敏,孟臣.数字式温湿度传感器及其应用技术[J].电子元器件应用,2014,19(8):136-139.

[4] 李泉溪.嵌入式原理及应用[M].北京:北京航天大学出版社,2019:41-48.

[5] 孙荣超,孙德超.数字温湿度数据记录仪的设计[J].现代电子技术,2015,7(12):56-61.

[6] 黄鸿,吴石增.传感器及其应用技术[M].北京:北京理工大学出版社,2018:26-32.

[7] 刘灿军.实用传感器[M].北京:国防工业出版社,2014:28-33.

[8] 孙惠芹.单片机项目设计教程[M].北京:电子工业出版社,2019:30-38.

[9] 宗光华,李大寨.多单片机系统应用技术[M].北京:国防工业出版社,2013:63-68.

[10] 王芳琴.单片机控制的节水灌溉系统的研究[J].华中农业大学,2016(16):81-88.

[11] 艾永乐,付子仪.数字电子技术基础[M].北京:中国电力出版社,2018:86-93.

[12] 陈根.互联网+智能家居:传统家居颠覆与重构[J].软件导刊,2020,10(02):212-213.

作者简介：

潘 宇(1988-)，男，硕士，讲师/工程师.研究领域:嵌入式系统开发，计算机应用.

张叶茂(1983-)，男，硕士，副教授/高级工程师.研究领域：智能控制技术.

莫淑贤(1987-)，女，硕士，讲师.研究领域:教育管理及信息化.本文通讯作者.