状态：受控

**密级：机密**

**日志系统2客户端日志接入**

**说明书**

|  |  |  |  |
| --- | --- | --- | --- |
| 文档编号： |  | | |
| 编 写： | 刘协雍 | 编写日期： | 2018/7/24 |
| 审 核： |  | 审核日期： |  |
| 批 准： |  | 批准日期： |  |

**修订状况**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **修订**  **章节** | **修订内容简述** | **修订**  **人员** | **修订**  **日期** | **修订后**  **版本号** | **批准人** |
|  | **升级2.0** | **刘协雍** | **2018/6/14** | **v2** |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**目 录**

[状态：受控 1](#_Toc516731457)

[1. 名词解释 3](#_Toc516731458)

[2. 总体说明 3](#_Toc516731459)

[2.1. preface 3](#_Toc516731460)

[2.2. 技术选型 3](#_Toc516731461)

[2.3. 主要技术考虑 3](#_Toc516731462)

[2.3.1. mq采用kafka 3](#_Toc516731463)

[2.3.2. 日志的收集采用filebeat 4](#_Toc516731464)

[~~2.3.3.~~ ~~日志落地采用文件方式~~ 4](#_Toc516731465)

[2.3.4. 日志落地采用HDFS文件方式 4](#_Toc516731466)

[2.3.5. 高并发日志收集 4](#_Toc516731467)

[2.3.6. 集群方案 4](#_Toc516731468)

[2.3.7. 关于系统分离 4](#_Toc516731469)

[2.3.8. 关于横向扩展 4](#_Toc516731470)

[3. 日志收集系统 4](#_Toc516731471)

[3.1. 系统架构图 5](#_Toc516731472)

[3.2. 系统安装 5](#_Toc516731473)

[3.2.1. 日志收集系统规划 5](#_Toc516731474)

[3.2.2. 组件及版本 5](#_Toc516731475)

[3.2.3. 组件下载 5](#_Toc516731476)

[3.2.4. 准备工作（三台服务器分别执行） 6](#_Toc516731477)

[3.2.5. Zookeeper配置 6](#_Toc516731478)

[3.2.6. Kafka 安装（在log2和log3中安装） 8](#_Toc516731479)

[3.2.7. Logstash 安装部署 10](#_Toc516731480)

[3.3. 系统监控 12](#_Toc516731481)

[3.4. 系统维护 12](#_Toc516731482)

[3.4.1. 常用命令 12](#_Toc516731483)

[3.5. 安全 12](#_Toc516731484)

[4. 日志调用接入 12](#_Toc516731485)

[4.1. beats 12](#_Toc516731486)

[4.1.1. 总述 12](#_Toc516731487)

[4.1.2. FileBeat centos7安装 12](#_Toc516731488)

[4.1.3. 配置使用 13](#_Toc516731489)

[4.1.4. 启动运行 13](#_Toc516731490)

[4.2. 高并发日志收集 13](#_Toc516731491)

[5. 日志分析 14](#_Toc516731492)

[5.1. 直通一体化操作及数据日志整合 14](#_Toc516731493)

[5.1.1. 逻辑处理架构图 14](#_Toc516731494)

[5.1.2. 业务处理流程图 14](#_Toc516731495)

[5.1.3. 总体设计考虑 14](#_Toc516731496)

[5.1.4. 详细设计 15](#_Toc516731497)

# 名词解释

|  |  |  |
| --- | --- | --- |
| **名称** | **说明** | **备注** |
|  |  |  |
|  |  |  |
|  |  |  |

# 总体说明

## preface

日志的接入，是指将业务的文档日志接入到日志中心系统。

# 业务系统接入改造

业务系统改造分为2种，初级改造和接口级改造，

这里先实现初级改造

## 初级改造

需要接入的系统，需要调整日志配置到：

1、需要配置到的日志文件夹，不包含其他无关内容，如果有其他无关内容，需要的配置中特殊处理（处理方式使用文件名匹配方式）

2、业务日志需要自身实现定期清理功能（清理周期为7天，自动清理7天前的日志文件）

PS：最好同时实现超过大小的自动清理

## 接口级改造

暂无

# 客户端安装

客户端安装基本分为windows和linux

## 基础要求

要求业务系统可以连到日志中心的mq服务器

## 红帽linux filebeats安装

mkdir -p /data/pack

cd /data/pack

wget <https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-5.5.2-x86_64.rpm>

rpm -vi filebeat-5.5.2-x86\_64.rpm

linux配置文件：

vim /etc/filebeat/filebeat.yml

## windows filebeats安装

1. Download the Filebeat Windows zip file from the downloads page.

2. Extract the contents of the zip file into C:\Program Files.

3. Rename the filebeat-<version>-windows directory to Filebeat.

4. Open a PowerShell prompt as an Administrator (right-click the PowerShell icon and select Run As Administrator).

From the PowerShell prompt, run the following commands to install Filebeat as a Windows service:

PS > cd 'C:\Program Files\Filebeat'

PS C:\Program Files\Filebeat> .\install-service-filebeat.ps1

配置文件为

filebeat.yml

## 修改配置

filebeat.prospectors:

- input\_type: log

paths:

- F:/temp/log/\*

encoding:GB2312

fields:

system\_id: apollo

multiline:

pattern: '^发生时间'

negate: true

match: after

output.kafka:

hosts: ["192.168.112.180:19092", "192.168.112.181:19092"]

topic: 'logHDFS'

key: 'apollo'

partition.hash:

hash: []

reachable\_only: true

required\_acks: 1

compression: gzip

max*\_message\_*bytes: 10000000



说明：

paths ：日志文件路径支持模糊匹配

system\_id：系统id

pattern：多行日志的开始匹配符号

key： 用于hash的值，一般取系统id

## 启动服务

sc start filebeat

或者

/etc/init.d/filebeat restart

## 设置为开机启动

略

# 监控

## filebeat监控

可以监控进程和服务状态

## 日志文件监控

设定长时间取值，判断是否有日志增加