Data Audit System Design

JSON API PART

Qu Qinglei 编写

quqinglei@icloud.com

2013 年 5 月

目录

1 插件管理

1.1 安装插件的命令

```
{
    "type": "addPlugin",
    "plugType": "parser",
}
```

安装插件的过程

(1) 在 WEBUI 端先上传插件，上传至/tmp/plugin/

(2) 执行安装插件命令，调用 python 安装脚本，python 程序先解包后释放到/opt/crouse/plugin

(3) 在数据库中添加这个插件的路径、名称、类型等

1.2 删除插件的命令

```
{
    "type": "removePlugin",
    "plugType": "parser",
    "plugName": "messagesParser",
    "dropDatabase": true
}
```

删除插件的过程

(1) 用户在 WEBUI 上找到删除插件功能，浏览插件

(2) 用户选择要删除的插件，然后按确定提交表单

(3) python 接收到删除插件的命令后会通知后台守护进程

(4) 后台守护进程会从内存中删掉插件，并从硬盘中删除该插件文件，并设置插件表为已删除

2 日志管理

2.1 添加监听日志的命令

```
{
    "type": "addDatatype",
```

```
    "dataType": "messages",
    "port": 514,
    "description": "about this kind of message, can be null."
}
```

过程

(1) 用户在配置中心找到“添加监听端口”，点击进入监听配置对话框

(2) 选择日志类型 → 填写监听端口 → 填写描述信息，可以不填写 → 点击确定

(3) python 在处理无误后发送命令给后台守护进程

(4) 后台会根据配置 fork 一个新的线程去监听此端口的日志，如果是插件支持的日志类型系统会自动启动插件

2.2 删除监听日志的命令

```
{
    "type": "removeDatatype",
    "dataType": "messages",
}
```

2.3 上传文件分析

```
{
    "type": "addData",
    "dataType": "messages",
}
```

上传文件以及后台执行过程

(1) 前台程序把日志数据上传至`/tmp/data/`

(2) 调用后台守护进程，fork 一个新的线程，读取文件并发送到 ømq[1]

(3) 线程处理完毕后会清空`/tmp/data/` 路径的所有内容

3 报警管理

3.1 添加报警条件的命令

```
{
    "type": "addAlarm",
    "alarmName": "Intrusion Detection",
    "dataType": "messages",
    "globalAlarm": false,
```

[1]我们统一把所有数据发送到 zeromq 进行统一处理

```
    "alarms": {
        "startTime": "2013-10-11:20:30:15",
        "endTime": "2013-10-11:20:30:15",
        "keywords": "attack#segment falt#stackoverflow#Job `cron.daily' terminated"
    }
}
```

3.2 删除报警条件的命令

```
{
    "type": "removeAlarm",
    "dataType": "messages",
    "alarmName": "Intrusion Detection"
}
```

4 过滤器管理

4.1 添加过滤器

```
{
    "type": "addFilter",
    "filterName": "useless",
    "dataType": "messages",
    "globalFilter": false,
    "filters": {
        "startTime": "2013-10-11:20:30:15",
        "endTime": "2013-10-11:20:30:15",
        "keywords": "useless#(CRON)#DHCPREQUEST"
    }
}
```

4.2 删除过滤器

```
{
    "type": "removeFilter",
    "filterName": "useless",
    "dataType": "messages"
}
```

5 邮箱配置管理

5.1 添加邮箱地址

```
{
    "type": "addEmail",
```

```
    "emailName": "quqinglei.aries@gmail.com",
    "mailCategory": "admin"
}
```

5.2 更改邮箱地址

```
{
    "type": "editEmail",
    "emailName": "quqinglei.aries@gmail.com",
}
```

5.3 删除邮箱地址

```
{
    "type": "removeEmail",
    "emailName": "quqinglei.aries@gmail.com",
}
```

6 数据管理

6.1 删除所有本地报警数据

```
{
    "type": "removeAllalarmData"
}
```

7 默认配置管理

7.1 设置数据保留的时间

```
{
    "type": "setDataRetentionTime",
    "last": 365
}
```

8 尾注

本文档主要涉及 JSON API 的设计格式，力求最简，在后期可能会有些改动，应该不大。版本更改内容会在尾注上标注。

Thu May 23 17:05:39 CST 2013 第一次编写