概述

一、相关组件介绍

1、Elastic Stack 包含：

- Beats 在这里是一个轻量级日志采集器，其实 Beats 家族有 6 个成员，早期的 ELK 架构中使用 Logstash 收集、解析日志，但是 Logstash 对内存、cpu、io 等资源消耗比较高。相比 Logstash，**Beats 所占系统的 CPU 和内存几乎可以忽略不计。**

  本次使用Metricbeat和Auditbeat进行数据采集：

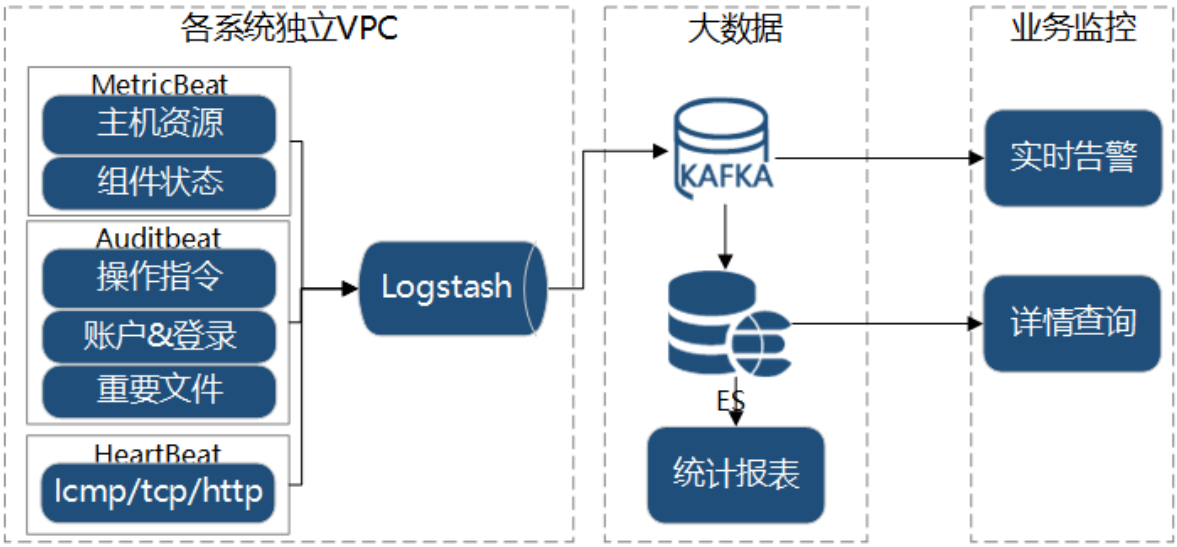
  - Metricbeat： 指标（收集系统、进程和文件系统级别的 CPU 和内存使用情况等数据）
  - Auditbeat：审计数据（收集审计日志）
  - Heartbeat：运行时间监控（收集系统运行时的数据）
- Logstash 主要是用来日志的搜集、分析、过滤日志的工具，支持大量的数据获取方式。一般工作方式为 c/s 架构，client 端安装在需要收集日志的主机上，server 端负责将收到的各节点日志进行过滤、修改等操作在一并发往 Elasticsearch 上去。
- Elasticsearch 是个开源分布式搜索引擎，提供搜集、分析、存储数据三大功能。它的特点有：分布式，零配置，自动发现，索引自动分片，索引副本机制，restful 风格接口，多数据源，自动搜索负载等。
- Kibana 也是一个开源和免费的工具，Kibana 可以为 Logstash 和 ElasticSearch 提供的日志分析友好的 Web 界面，可以帮助**汇总、分析和搜索重要数据日志。**

2、Grafana是一个跨平台的开源的度量分析和可视化工具，可以通过将采集的**数据查询然后可视化的展示，并及时通知。**

3、ClusterShell轻量级的集群管理工具，原理是利用ssh，可以说是Linux系统下非常好用的运维利器。

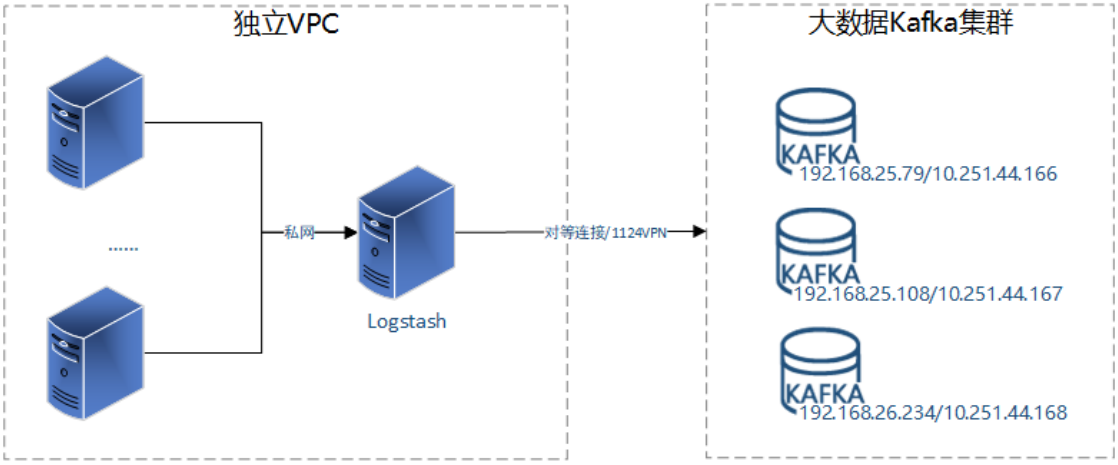
二、总体架构

流程示意图



部署说明

1. 各系统在每台被监控主机部署Metricbeat、Auditbeat进行基本信息采集；
2. 每个系统在独立的VPC中部署一台Logstash，实现数据汇聚，对接大数据平台的kafka集群；
3. Logstash部署主机要求：
    - 集群内主机，与集群内所有主机通信，做好访问策略控制。
    - 申请低配主机，单独部署Logstash进程，无其他应用。
    - 统一安装Linux操作系统，版本为CentOS 7.2。
    - 与大数据平台kafka集群通信，已建立对等连接通过私网地址访问，否则通过1124VPN访问，调通网络，并做好访问策略控制。



三、监控内容说明

- 主机资源采集内容（Metricbeat）
    - 监测内容：内存、CPU、文件系统、网络IO
    - 采集周期五分钟
- 审计信息采集内容（Auditbeat）
    - 命令审计：mkfs|dd|rm|mv|wget
    - 用户账户审计：用户的添加、删除、属性修改
    - 用户登录审计
    - 重要目录文件审计：created|deleted|moved|updated
- 主机之间通信情况监测
- 基本信息包含以下内容
    - 所在节点（如苏州云等），VPC，系统名称，主机的IP、MAC

安装及说明

一、安装软件列表

软件	版本	说明
JDK	1.8以上	
ClusterShell	1.7.3	集群管理工具
Metricbeat	6.5.4	主机资源采集
Auditbeat	6.5.4	审计信息采集
Heartbeat	6.5.4	系统运行监测
Logstash	6.2.4	日志收集、过滤、转发

二、ClusterShell安装

Clustershell作用说明： 1、向集群中的节点分发文件 2、向集群中的节点下发命令

前言：

在使用clustershell前，需要先配置ssh免密登陆。例如现有集群，包括三个节点A，B，C。其中clustershell部署在A节点上。 那么需分别配置A节点到自身的免密登陆；A到B的免密登陆；A到C的免密登陆。

一）免密登陆的配置

Steps:

1、在用户的home目录(进入用户home目录），进入.ssh目录（如果没有则新建.ssh, mkdir .ssh),

使用下面的语句，生成公钥和私钥：

```
shell>  ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:uoANROmy5U5DUbc4WTdOBks67uB+AlIwwJvTHqC1eJs root@ecs-831b-
0703885.novalocal
The key's randomart image is:
+---[RSA 2048]----+
|o.. =o. o.*.o    |
| o+B . = = =     |
|.o*+* + + .      |
|o+o*.. o .       |
| .+++ . S        |
|  E*.. +         |
|  ..o.o .        |
|     o...        |
|      oo         |
+----[SHA256]-----+
```

2、进入.ssh目录，用下面的语句将公钥上传到需要免密登陆的节点上。例如上将公钥上传到B节点（用户userB）：

> ssh-copy-id -i id_rsa.pub userB@B_ip

3、检验免密登陆是否设置成功：

> ssh userB@B_ip

如果执行该语句后，不需要输入密码就进入了B，那么免密登陆设置成功。

二) Clustershell 配置及文件下发

Steps：

1、配置了一个集群，例如集群名称为cluster_demo,集群中包含了三个节点A、B、C使用下面的语句：

```
shell> vi /etc/clustershell/groups
cluster_demo: A_IP B_IP C_IP
```

2、检测集群是否配置成功，使用nodeset -ll，查看是否有cluster_demo集群名称，有则成功。

3、利用clush命令，向集群下的节点分发文件。例如分发home下的auditbeat-6.5.4-linux-x86_64.tar.gz文件， 到集群的节点下的dir目录。命令如下：

```
# 分发文件
clush -g cluster_demo -c /home/auditbeat-6.5.4-linux-x86_64.tar.gz --dest /dir
```

三、beats安装

1、Metricbeat安装

Steps:

1、下载安装包:

```
https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.5.4-linux-x86_64.tar.gz
```

2、通过上述的clush命令将该压缩文件下发到集群下的各个节点上。

3、解压

```
tar xvf metricbeat-6.5.4-linux-x86_64.tar.gz
```

4、修改metricbeat.yml

```
#========================  Modules configuration ============================

metricbeat.config.modules:
  # Glob pattern for configuration loading
  path: ${path.config}/modules.d/system.yml

  # Set to true to enable config reloading
  reload.enabled: true

  # Period on which files under path should be checked for changes
  reload.period: 60s

#================================ General =====================================
```

```
# Optional fields that you can specify to add additional information to the
# output.
fields:
  system: test
  type: metric
  vpc: 899d1aef-902a-4cfb-8ec3-8630054c0809
  location: 苏州云

#================================ Outputs =====================================
#-------------------------- Logstash output -------------------------------
output.logstash:
  # The Logstash hosts  根据实际情况修改
  hosts: ["localhost:5044"]

#================================ Procesors
=====================================
# Configure processors to enhance or manipulate events generated by the beat.
processors:
  - add_host_metadata:
    netinfo.enabled: true
processors:
  - add_cloud_metadata: ~
```

备注：各系统务必根据实际情况修改**fields.type、fields.system、fields.vpc、fiels.location**字段

修改modules.d/system.yml，增加获取主机ip、mac信息的功能，修改后的内容为

```
- module: system
  period: 5m
  metricsets:
    - cpu
    #- load
    - memory
    - network
    #- process
    - process_summary
    #- core
    #- diskio
    #- socket
  process.include_top_n:
    by_cpu: 5      # include top 5 processes by CPU
    by_memory: 5   # include top 5 processes by memory

- module: system
  period: 5m
  metricsets:
    - filesystem
    - fsstat
  processors:
  - drop_event.when.regexp:
      system.filesystem.mount_point: '^/(sys|cgroup|proc|dev|etc|host|lib)($|/)'
```

5、启动

```
./metricbeat &
```

2、Auditbeat安装

Steps:

1、下载安全包，路径：

```
https://artifacts.elastic.co/downloads/beats/auditbeat/auditbeat-6.5.4-linux-
x86_64.tar.gz
```

2、通过上述的clush命令将该压缩文件下发到集群下的各个节点上。

3、解压

```
tar xvf auditbeat-6.5.4-linux-x86_64.tar.gz
```

4、修改auditbeat.yml

```
#==========================  Modules configuration ============================
auditbeat.modules:

- module: auditd
  # Load audit rules from separate files. Same format as audit.rules(7).
  audit_rule_files: [ '${path.config}/audit.rules.d/sample-rules-linux-
64bit.conf']
- module: file_integrity
  paths:
  - /bin
  - /usr/bin
  - /sbin
  - /usr/sbin
  - /etc

#================================ General =====================================
# Optional fields that you can specify to add additional information to the
# output.    根据实际情况修改
fields:
  system: test
  type: audit
  vpc: 899d1aef-902a-4cfb-8ec3-8630054c0809
  location:苏州云

#================================ Outputs =====================================
#-------------------------- Logstash output ------------------------------
output.logstash:
  # The Logstash hosts   根据实际情况修改
  hosts: ["localhost:5044"]

#================================ Procesors
=====================================
# Configure processors to enhance or manipulate events generated by the beat.
processors:
  - add_host_metadata:
    netinfo.enabled: true
processors:
  - add_cloud_metadata: ~
```

备注：各系统务必根据实际情况修改**fields.type、fields.system、fields.vpc、fiels.location**字段

修改sample-rules-linux-64bit.conf

```
## If you are on a 64 bit platform, everything should be running
## in 64 bit mode. This rule will detect any use of the 32 bit syscalls
## because this might be a sign of someone exploiting a hole in the 32
## bit API.
#-a always,exit -F arch=b32 -S all -F key=32bit-abi

## Executions.
-a always,exit -F arch=b64 -S execve,execveat -k exec

## External access (warning: these can be expensive to audit).
-a always,exit -F arch=b64 -S accept,bind,connect -F key=external-access

## Identity changes.
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity

## Unauthorized access attempts.
-a always,exit -F arch=b64 -S
open,creat,truncate,ftruncate,openat,open_by_handle_at -F exit=-EACCES -k access
-a always,exit -F arch=b64 -S
open,creat,truncate,ftruncate,openat,open_by_handle_at -F exit=-EPERM -k access
```

5、查看规则

```
./auditbeat show auditd-rules
```

6、启动

```
./auditbeat &
```

3、Heartbeat

Steps:

1、下载安装包

```
https://artifacts.elastic.co/downloads/beats/heartbeat/heartbeat-6.5.4-linux-
x86_64.tar.gz
```

2、通过上述的clush命令将该压缩文件下发到集群下的各个节点上。

3、解压

```
tar xvf heartbeat-6.5.4-linux-x86_64.tar.gz
```

4、修改heartbeat.yml

```
############################# Heartbeat ######################################
heartbeat.monitors:
```

```
- type: icmp # monitor type `icmp` (requires root) uses ICMP Echo Request to
ping
             # configured hosts

  # Configure task schedule using cron-like syntax
  schedule: '@every 300s'

  # List of hosts to ping
  hosts: ["localhost"]

  # Configure IP protocol types to ping on if hostnames are configured.
  # Ping all resolvable IPs if `mode` is `all`, or only one IP if `mode` is
`any`.
  ipv4: true
  ipv6: true
  mode: all

  # Total running time per ping test.
  timeout: 16s

  # Waiting duration until another ICMP Echo Request is emitted.
  wait: 1s

#================================ General =====================================
# Optional fields that you can specify to add additional information to the
# output.   根据实际情况修改
fields:
  system: test
  type: heart
  vpc: 899d1aef-902a-4cfb-8ec3-8630054c0809
  location: 苏州云


#================================ Outputs =====================================
#-------------------------- Logstash output -------------------------------
output.logstash:
  # The Logstash hosts  根据实际情况修改
  hosts: ["localhost:5044"]

#================================ Procesors
=====================================
# Configure processors to enhance or manipulate events generated by the beat.
processors:
  - add_host_metadata:
    netinfo.enabled: true
processors:
  - add_cloud_metadata: ~
```

备注：各系统务必根据实际情况修改**fields.type、fields.system、fields.vpc、fiels.location**字段

5、启动

> ./heartbeat &

四、Logstash安装

1、下载安装包，路径：

```
https://artifacts.elastic.co/downloads/logstash/logstash-6.2.4.tar.gz
```

2、解压

```
tar xvf logstash-6.2.4.tar.gz
```

3、修改logstash.conf

```
shell>cp logstash-sample.conf logstash.conf
shell>vi logstash.conf
input {
  beats {
    port => 5044
  }
}


#输出到kafka
output{
    kafka{
       acks => "1"
       topic_id => "topic_lx_wss"
       bootstrap_servers =>
["192.168.25.79:8092,192.168.25.108:8092,192.168.26.234:8092"]
       codec => "json"
       retries => 0
       request_timeout_ms => "10000"
       batch_size => 1
       security_protocol => "SSL"
       ssl_keystore_location => "/home/zn/logstash-
6.5.4/config/jks/lx_wss/lx_wss.keystore.jks"
       ssl_keystore_password => "OQRLzxY34sJ11HRs"
       ssl_truststore_location => "/home/zn/logstash-
6.5.4/config/jks/lx_wss/lx_wss.truststore.jks"
       ssl_truststore_password => "OQRLzxY34sJ11HRs"
  }
}
```

ps: kafka具体连接方式会通过邮件单独发送

4、启动

```
./logstash -f ../config/logstash.conf  &
```

各系统分配的fields.system、kafka topic如下：

fields.system	Topic	metric索引名	audit索引名	heart索引名
unionapp	topic_unionapp	unionapp_metric_yyyyMMdd	unionapp_audit_yyyyMMdd	unionapp_heart_yyyyMMdd
cardmanagment	topic_cardmanagment	cardmanagment_metric_yyyyMMdd	cardmanagment_audit_yyyyMMdd	cardmanagment_heart_yyyyMMdd
trace	topic_trace	trace_metric_yyyyMMdd	trace_audit_yyyyMMdd	trace_heart_yyyyMMdd
certification	topic_certification	certification_metric_yyyyMMdd	certification_audit_yyyyMMdd	certification_heart_yyyyMMdd
dcp	topic_dcp	dcp_metric_yyyyMMdd	dcp_audit_yyyyMMdd	dcp_heart_yyyyMMdd
sms	topic_sms	sms_metric_yyyyMMdd	sms_audit_yyyyMMdd	sms_heart_yyyyMMdd
simulator	topic_simulator	simulator_metric_yyyyMMdd	simulator_audit_yyyyMMdd	simulator_heart_yyyyMMdd
producehelp	topic_producehelp	producehelp_metric_yyyyMMdd	producehelp_audit_yyyyMMdd	producehelp_heart_yyyyMMdd
monitor	topic_monitor	monitor_metric_yyyyMMdd	monitor_audit_yyyyMMdd	monitor_heart_yyyyMMdd
lx_wss	topic_lx_wss	lx_wss_metric_yyyyMMdd	lx_wss_audit_yyyyMMdd	lx_wss_heart_yyyyMMdd
yx_wss	topic_yx_wss	yx_wss_metric_yyyyMMdd	yx_wss_audit_yyyyMMdd	yx_wss_heart_yyyyMMdd
aep	topic_aep	aep_metric_yyyyMMdd	aep_audit_yyyyMMdd	aep_heart_yyyyMMdd

五、JDK安装说明

Steps：

1、下载JDK安装包linux版本64位，版本要求jdk1.8版本以上。

2、在/usr/local下创建java文件夹，指令如下：

1）cd /usr/local 2) mkdir java

3、将离线安装包拷贝到Step 2创建的java文件中。此处分情况拷贝：

1）linux端到端的拷贝，例如拷贝文件到ip2（用户名user2）。参考该命令： scp user2@ip2:/dir/ 具体用法参考linux shell教程 scp命令。 2）如果将文件file1分发到集群的各个节点上（集群名称cluster_demo)的dir目录中。先进入file所在的文件夹。参考该命令： clush -g cluster_demo -c file1 --dest /dir

4、解压jdk压缩文件： tar xvf filename.tar.gz

5、执行下面的命令：

1) update-alternatives --install "usr/bin/java" "java" "/usr/loca/java/jdk_version/bin/java" 1 2) update-alternatives --install "usr/bin/javac" "javac" "/usr/loca/java/jdk_version/bin/javac" 1 3) update-alternatives --install "usr/bin/javaws" "java" "/usr/loca/java/jdk_version/bin/javaws" 1

6、在命令行中输入java 回车、javac 回车。检验是否有输出，有输出则为安装成功。