收集Nginx日志

2016年10月19日

10:27

**Logstash配置**

**/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-patterns-core-2.0.5/patterns/nginx**

NGUSERNAME [a-zA-Z\.\@\-\+\_%]+

NGUSER %{NGUSERNAME}

SAPPACCESS (%{NOTSPACE:ClientIP},|-) (%{NOTSPACE:Aligaofang} -|-) (%{IPORHOST:Aliwaf} -|-) %{IPORHOST:http\_host} - %{NOTSPACE:remote\_user} \[%{HTTPDATE:timestamp}\] \"(?:%{WORD:verb} %{NOTSPACE:request}(?: HTTP/%{NUMBER:httpversion})?|%{DATA:rawrequest})\" %{NUMBER:response} (?:%{NUMBER:bytes}|-) %{QS:referrer} %{QS:agent} (%{NUMBER:time\_duration:float}|-) (?:%{NUMBER:time\_backend\_response:float}|-)

<<nginx\_logs.conf>>

**/etc/logstash/conf.d/nginx\_logs.conf**

input {

redis {

batch\_count => 1

host => "100.114.75.63"

port => "6379"

db => "12"

data\_type => "list"

password => "1acda2f7e2b54a31:dK5mGZ9yUwsg"

key => "www-access-log"

type => "www-access-log"

}

redis {

batch\_count => 1

host => "100.114.75.63"

port => "6379"

db => "12"

data\_type => "list"

password => "1acda2f7e2b54a31:dK5mGZ9yUwsg"

key => "swww-access-log"

type => "swww-access-log"

}

redis {

batch\_count => 1

host => "100.114.75.63"

port => "6379"

db => "12"

data\_type => "list"

password => "1acda2f7e2b54a31:dK5mGZ9yUwsg"

key => "app-access-log"

type => "app-access-log"

}

redis {

batch\_count => 1

host => "100.114.75.63"

port => "6379"

db => "12"

data\_type => "list"

password => "1acda2f7e2b54a31:dK5mGZ9yUwsg"

key => "sapp-access-log"

type => "sapp-access-log"

}

redis {

batch\_count => 1

host => "100.114.75.63"

port => "6379"

db => "12"

data\_type => "list"

password => "1acda2f7e2b54a31:dK5mGZ9yUwsg"

key => "wx-access-log"

type => "wx-access-log"

}

redis {

batch\_count => 1

host => "100.114.75.63"

port => "6379"

db => "12"

data\_type => "list"

password => "1acda2f7e2b54a31:dK5mGZ9yUwsg"

key => "swx-access-log"

type => "swx-access-log"

}

}

filter {

grok {

match => { "message" => "%{NGINXACCESS}" }

}

if ([message] =~ "^-") {

drop {}

}

geoip {

source => "ClientIP"

target => "geoip"

database => "/etc/logstash/GeoLite2-City.mmdb"

add\_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]

add\_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}" ]

}

mutate {

convert => [ "[geoip][coordinates]", "float" ]

}

}

output {

if [type] == "www-access-log" {

elasticsearch {

hosts => ["10.171.60.25:9200"]

index => "logstash-www-access-log-%{+YYYY-MM-dd}"

}

}

if [type] == "swww-access-log" {

elasticsearch {

hosts => ["10.171.60.25:9200"]

index => "logstash-swww-access-log-%{+YYYY-MM-dd}"

}

}

if [type] == "app-access-log" {

elasticsearch {

hosts => ["10.171.60.25:9200"]

index => "logstash-app-access-log-%{+YYYY-MM-dd}"

}

}

if [type] == "sapp-access-log" {

elasticsearch {

hosts => ["10.171.60.25:9200"]

index => "logstash-sapp-access-log-%{+YYYY-MM-dd}"

}

}

if [type] == "wx-access-log" {

elasticsearch {

hosts => ["10.171.60.25:9200"]

index => "logstash-wx-access-log-%{+YYYY-MM-dd}"

}

}

if [type] == "swx-access-log" {

elasticsearch {

hosts => ["10.171.60.25:9200"]

index => "logstash-swx-access-log-%{+YYYY-MM-dd}"

}

}

}

**Nginx---Logstash配置**

input {

file {

path => ["/app/nginx/logs/sapp\_access.log"]

type => "sapp-access-log"

start\_position => "beginning"

}

file {

path => ["/app/nginx/logs/swww\_access.log"]

type => "swww-access-log"

start\_position => "beginning"

}

file {

path => ["/app/nginx/logs/www\_access.log"]

type => "www-access-log"

start\_position => "beginning"

}

file {

path => ["/app/nginx/logs/wx\_access.log"]

type => "wx-access-log"

start\_position => "beginning"

}

file {

path => ["/app/nginx/logs/app\_access.log"]

type => "app-access-log"

start\_position => "beginning"

}

file {

path => ["/app/nginx/logs/file\_access.log"]

type => "file-access-log"

start\_position => "beginning"

}

}

filter {

}

output {

if [type] == "sapp-access-log" {

redis {

host => "10.26.250.198"

port => "6379"

db => "1"

password => "5ef16d1844774cc8:B7Z15ICUF3e43v1j0GwMZixkunAQ3f"

data\_type => "list"

key => "sapp-access-log"

workers => 10

}

}

if [type] == "swww-access-log" {

redis {

host => "10.26.250.198"

port => "6379"

db => "1"

password => "5ef16d1844774cc8:B7Z15ICUF3e43v1j0GwMZixkunAQ3f"

data\_type => "list"

key => "swww-access-log"

workers => 10

}

}

if [type] == "www-access-log" {

redis {

host => "10.26.250.198"

port => "6379"

db => "1"

password => "5ef16d1844774cc8:B7Z15ICUF3e43v1j0GwMZixkunAQ3f"

data\_type => "list"

key => "www-access-log"

workers => 10

}

}

if [type] == "wx-access-log" {

redis {

host => "10.26.250.198"

port => "6379"

db => "1"

password => "5ef16d1844774cc8:B7Z15ICUF3e43v1j0GwMZixkunAQ3f"

data\_type => "list"

key => "wx-access-log"

workers => 10

}

}

if [type] == "app-access-log" {

redis {

host => "10.26.250.198"

port => "6379"

db => "1"

password => "5ef16d1844774cc8:B7Z15ICUF3e43v1j0GwMZixkunAQ3f"

data\_type => "list"

key => "app-access-log"

workers => 10

}

}

if [type] == "file-access-log" {

redis {

host => "10.26.250.198"

port => "6379"

db => "1"

password => "5ef16d1844774cc8:B7Z15ICUF3e43v1j0GwMZixkunAQ3f"

data\_type => "list"

key => "file-access-log"

workers => 10

}

}

}

**Nginx配置文件log字段**

log\_format main '$http\_x\_forwarded\_for - $remote\_addr - $server\_name - $remote\_user [$time\_local] "$request" '

'$status $body\_bytes\_sent "$http\_referer" '

'"$http\_user\_agent" $request\_time $upstream\_response\_time';

log\_format main '$http\_x\_forwarded\_for - $remote\_addr - $server\_name - $remote\_user [$time\_local] "$request" '

'$status $body\_bytes\_sent "$http\_referer" '

'"$http\_user\_agent" $request\_time $upstream\_response\_time';