**시스템 설치 환경 파일**

Nginx /usr/local/nginx/conf

/etc/rc.d/init.d/nginx start|stop|configtest (구동)

Fluentd : /etc/fluentd

/etc/rc.d/init.d/td-agent start|stop|configtest (구동)

Td-agent /etc/td-agent

/etc/rc.d/init.d/ td-agent start|stop|configtest (구동)

Elastic /data/logmon/elasticsearch2/

/etc/elasticsearch/elasticsearch.yml

/etc/sysconfig/elasticsearch (변수)

/etc/rc.d/init.d/elasticsearch start|stop|configtest (구동)

|  |
| --- |
| [root@dev1 nginx]# pstree -A  init-+-acpid  |-crond  |-java---49\*[{java}]  |-java---37\*[{java}]  |-login---bash  |-5\*[mingetty]  |-mysqld\_safe---mysqld---21\*[{mysqld}]  **|-nginx---2\*[nginx]**  **|-php-fpm---2\*[php-fpm]**  |-redis-server---2\*[{redis-server}]  |-rsyslogd---3\*[{rsyslogd}]  **|-ruby-+-ruby---9\*[{ruby}]**  **| `-{ruby}**  |-2\*[sendmail]  |-smbd---smbd  |-snmpd  |-sshd---sshd---bash---pstree  |-udevd---2\*[udevd]  `-xinetd |

|  |
| --- |
| **[root@dev1 nginx]# netstat -natp**  **[root@dev1 nginx]# netstat -natp | sed -e"s/ / /g"| sort -k 7**  Active Internet connections (servers and established)  tcp 0 0 127.0.0.1:8888 0.0.0.0:\* LISTEN 1427/php-fpm  tcp 0 0 0.0.0.0:6379 0.0.0.0:\* LISTEN 1437/redis-server  tcp 0 0 127.0.0.1:199 0.0.0.0:\* LISTEN 1457/snmpd  tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 1469/sshd  tcp 0 0 :::22 :::\* LISTEN 1469/sshd  tcp 0 0 :::2401 :::\* LISTEN 1477/xinetd  tcp 0 0 :::873 :::\* LISTEN 1477/xinetd  tcp 0 0 :::3306 :::\* LISTEN 1816/mysqld  tcp 0 0 0.0.0.0:25 0.0.0.0:\* LISTEN 1862/sendmail  tcp 0 0 0.0.0.0:24220 0.0.0.0:\* LISTEN 18756/ruby  tcp 0 0 0.0.0.0:9999 0.0.0.0:\* LISTEN 18756/ruby  tcp 0 0 127.0.0.1:24224 0.0.0.0:\* LISTEN 18756/ruby  tcp 0 0 127.0.0.1:24230 0.0.0.0:\* LISTEN 18756/ruby  tcp 0 0 0.0.0.0:139 0.0.0.0:\* LISTEN 19125/smbd  tcp 0 0 0.0.0.0:445 0.0.0.0:\* LISTEN 19125/smbd  tcp 0 0 0.0.0.0:80 0.0.0.0:\* LISTEN 1932/nginx  tcp 0 0 0.0.0.0:8081 0.0.0.0:\* LISTEN 1932/nginx  tcp 0 0 0.0.0.0:8085 0.0.0.0:\* LISTEN 1932/nginx  tcp 0 0 0.0.0.0:9290 0.0.0.0:\* LISTEN 1932/nginx  tcp 0 0 0.0.0.0:9990 0.0.0.0:\* LISTEN 1932/nginx  tcp 0 0 10.20.10.240:9200 0.0.0.0:\* LISTEN 6818/java  tcp 0 0 10.20.10.240:9300 0.0.0.0:\* LISTEN 6818/java  tcp 0 0 0.0.0.0:26489 0.0.0.0:\* LISTEN 8147/java  tcp 0 0 10.20.10.240:1337 0.0.0.0:\* LISTEN 8147/java  tcp 0 0 127.0.0.1:7473 0.0.0.0:\* LISTEN 8147/java  tcp 0 0 127.0.0.1:7474 0.0.0.0:\* LISTEN 8147/java  tcp 0 0 127.0.0.1:7687 0.0.0.0:\* LISTEN 8147/java  tcp 0 96 10.20.10.240:22 10.20.10.108:59365 ESTABLISHED 903/sshd  Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name |

Nginx

|  |
| --- |
| **[root@dev1 conf]# cat nginx.conf**  #user nobody;  worker\_processes 2;  events {  worker\_connections 8096;  multi\_accept on;  use epoll;  }  worker\_rlimit\_nofile 40000;  #error\_log logs/error.log;  #error\_log logs/error.log info;  error\_log logs/error.log notice;  #pid logs/nginx.pid;  # for WEB Server  **include nginx\_http.conf;** |

|  |
| --- |
| [root@dev1 conf]# cat **nginx\_http.conf**  http {  include mime.types;  default\_type application/octet-stream;  log\_format main '$remote\_addr - $remote\_user [$time\_local] "$request" '  '$status $body\_bytes\_sent "$http\_referer" '  '"$http\_user\_agent" "$http\_x\_forwarded\_for"';  access\_log logs/access.log ;  sendfile on;  tcp\_nopush on;  tcp\_nodelay on;  gzip on;  gzip\_disable "msie6";  keepalive\_timeout 25;  # this is where you define your clusters.  upstream es\_search\_9200 {  server 10.20.10.240:9200 max\_fails=3 fail\_timeout=30s;  server 10.20.10.240:9200 backup;  }  upstream fluent\_log\_9999 {  server 10.20.10.240:9999 max\_fails=3 fail\_timeout=30s;  server 10.20.10.240:9999 backup;  }  #-----------------------------------------------------------------------  include "default/vhost\_default.conf"; # listen 80,sample,443  # elastic  include "logminor/vhost\_kibana.conf"; # listen 8085; /data/logminor/kibana3  include "logminor/vhost\_esch.conf"; # listen 9290 -> 9200;  **include "logminor/vhost\_fluent.conf"**; # listen 9990 -> 9999;  include "CORONA/vhost\_corona.conf"; # listen 8081; /svc/web\_app/CORONA;  } |

|  |
| --- |
| **[root@dev1 conf]# cat logminor/vhost\_fluent.conf**  server {  listen 9990;  server\_name eslog.im.com 10.20.10.240;  charset UTF-8*;*  access\_log logs/access-logmon\_eslog.log;  error\_log logs/error-logmon\_eslog.log;  add\_header 'Access-Control-Allow-Origin' '\*';  add\_header 'Access-Control-Allow-Credentials' 'true';  add\_header 'Access-Control-Allow-Methods' 'GET,POST,DELETE';  location ~ / {  return 204;  }  location ~ ^/\*.action {  # proxy\_pass http://192.168.28.165:9999;  proxy\_pass http://fluent\_log\_9999/$2;  proxy\_read\_timeout 90;  }  location ~ ^/\* {  # proxy\_pass http://192.168.28.165:9999;  proxy\_pass http://fluent\_log\_9999/$2;  proxy\_read\_timeout 90;  }  # redirect server error pages to the static page /50x.html  # nginx html  error\_page 404 /404.html;  error\_page 500 502 503 504 /50x.html;  location = /50x.html {  root /usr/local/nginx/html;  }  } |

|  |
| --- |
| [root@dev1 conf]# cat **logminor/vhost\_esch.conf**  server {  listen 9290;  server\_name es.im.com 10.20.10.240;  charset UTF-8*;*  access\_log logs/access-logmon\_eslog.log;  error\_log logs/error-logmon\_eslog.log;  add\_header 'Access-Control-Allow-Origin' '\*';  add\_header 'Access-Control-Allow-Credentials' 'true';  add\_header 'Access-Control-Allow-Methods' 'GET,POST,HEAD,DELETE,PUT,OPTIONS';  # For CORS Ajax  proxy\_pass\_header Access-Control-Allow-Origin;  proxy\_pass\_header Access-Control-Allow-Methods;  proxy\_hide\_header Access-Control-Allow-Headers;  add\_header Access-Control-Allow-Headers 'X-Requested-With, Content-Type';  add\_header Access-Control-Allow-Credentials true;  location ~ ^/cbt\* {  proxy\_pass http://es\_search\_9200;  proxy\_read\_timeout 90;  }  location ~ ^/es\* {  proxy\_pass http://es\_search\_9200;  proxy\_read\_timeout 90;  }  location ~ ^/\_plugin\* {  proxy\_pass http://es\_search\_9200;  proxy\_read\_timeout 90;  }  location ~ ^/\* {  proxy\_pass http://es\_search\_9200;  proxy\_read\_timeout 90;  }  # redirect server error pages to the static page /50x.html  error\_page 404 /404.html;  error\_page 500 502 503 504 /50x.html;  location = /50x.html {  root /usr/local/nginx/html;  }  } |

|  |
| --- |
| [root@dev1 conf]# cat logminor/vhost\_kibana.conf  server {  listen 8085;  server\_name 10.20.10.240 logmon.im.com kibana.interpark.com;  #charset koi8-r;  access\_log logs/access-logmon\_kibana.log;  error\_log logs/error-logmon\_kibana.log;  **root /data/logminor/kibana3;**  location / {  root /data/logminor/kibana3;  index index.html index.htm;  }  add\_header 'Access-Control-Allow-Origin' '\*';  add\_header 'Access-Control-Allow-Credentials' 'true';  add\_header 'Access-Control-Allow-Methods' 'GET,POST,HEAD,DELETE,PUT,OPTIONS';  # pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000  location ~ \.(php|html|inc)$ {  # root /data/logminor/kibana3;  try\_files $uri /index.php =404;  fastcgi\_pass 127.0.0.1:8888;  fastcgi\_index index.php;  fastcgi\_param SCRIPT\_FILENAME $document\_root$fastcgi\_script\_name;  include fastcgi\_params;  }  location ~ ^/\_aliases$ {  proxy\_pass http://es\_search\_9200;  proxy\_read\_timeout 90;  proxy\_set\_header Host $host;  proxy\_set\_header X-Real-IP $remote\_addr;  proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;  }  location ~ ^/.\*/\_aliases$ {  #proxy\_pass http://127.0.0.1:9200;  proxy\_pass http://es\_search\_9200;  proxy\_read\_timeout 90;  proxy\_set\_header Host $host;  proxy\_set\_header X-Real-IP $remote\_addr;  proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;  }  location ~ ^/\_nodes$ {  proxy\_pass http://es\_search\_9200;  proxy\_read\_timeout 90;  proxy\_set\_header Host $host;  proxy\_set\_header X-Real-IP $remote\_addr;  proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;  }  location ~ ^/.\*/\_search$ {  proxy\_pass http://es\_search\_9200;  proxy\_read\_timeout 90;  proxy\_set\_header Host $host;  proxy\_set\_header X-Real-IP $remote\_addr;  proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;  }  location ~ ^/.\*/\_mapping {  proxy\_pass http://es\_search\_9200;  proxy\_read\_timeout 90;  proxy\_set\_header Host $host;  proxy\_set\_header X-Real-IP $remote\_addr;  proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;  }  # redirect server error pages to the static page /50x.html  error\_page 404 /404.html;  error\_page 500 502 503 504 /50x.html;  location = /50x.html {  root /usr/local/nginx/html;  }  } |

|  |
| --- |
| [root@dev1 td-agent]# cat td-agent.conf  ## built-in TCP input  ## $ echo <json> | fluent-cat <tag>  <source>  @type forward  bind 127.0.0.1  port 24224  </source>  ## built-in UNIX socket input  #<source>  # @type unix  #</source>  # HTTP input  # http://localhost:9999/<tag>?json=<json>  <source>  @type http  port 9999  bind 0.0.0.0  body\_size\_limit 32m  keepalive\_timeout 10s  </source>  ## File input  ## read apache logs with tag=apache.access  #<source>  # @type tail  # format apache  # path /var/log/httpd-access.log  # tag apache.access  #</source>  # Listen HTTP for monitoring  # http://localhost:24220/api/plugins  # http://localhost:24220/api/plugins?type=TYPE  # http://localhost:24220/api/plugins?tag=MYTAG  <source>  @type monitor\_agent  port 24220  </source>  # Listen DRb for debug  <source>  @type debug\_agent  bind 127.0.0.1  port 24230  </source>  #################################  ## Output descriptions:  #################################  # \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  # HTTP\_LOCAL ## File input  # @include fluent\_httpd.conf  ## \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  ## elasticsearch  # @include /etc/td-agent/es/fluent\_elasticsearch.conf  # @include /etc/td-agent/shop/fluent\_shop.action\_es.conf  # @include /etc/td-agent/shop/fluent\_shop.action\_mysql.conf  @include /etc/td-agent/action/fluent\_test2.action.conf  @include /etc/td-agent/action/fluent\_test2.action\_es\_mysql.conf  # @include /etc/td-agent/address/fluent\_annotation.conf  # @include /etc/td-agent/address/fluent\_address.conf  # @include /etc/td-agent/test/fluent\_test.conf  ## Common  ## \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  <match alert.\*\*>  @type file  path /var/log/td-agent/alerts  </match>  <match debug.\*\*>  @type stdout  @log\_level debug  </match>  #<match \*\*>  # @type blackhole\_plugin  #</match> |

|  |
| --- |
| [root@dev1 td-agent]# cat /etc/td-agent/action/fluent\_test2.action.conf  <match test2.action.\*\*>  @type file  path /data/logminor/TD\_LOGS/test2.action/test2.action  # -- test2.action.20160118.log  # time\_slice\_format %Y%m%d  # -- test2.action.201601181401.log  time\_slice\_format %Y%m%d%H%M  append true  format json  include\_time\_key true  time\_key time\_key  buffer\_type file  buffer\_path /var/log/td-agent/buffer/test2\_action\_in.buffer  # flush\_at\_shutdown true  # flush\_interval 20s # for testing  flush\_interval 20s  retry\_limit 7  retry\_wait 10s  num\_threads 2  </match> |

|  |
| --- |
| [root@dev1 td-agent]# cat /etc/td-agent/action/fluent\_test2.action\_es\_mysql.conf  <source>  @type tail  # path /data/logminor/TD\_LOGS/test2.action/test2.action.%Y%m%d.[a-zA-Z]\*  # --> test2.action.201601181400.log  # path /data/logminor/TD\_LOGS/test2.action/test2.action.%Y%m%d%H%M\*.log # nolog append  # --> test2.action.20160118.log  path /data/logminor/TD\_LOGS/test2.action/test2.action.%Y%m%d\*  pos\_file /var/log/td-agent/fw.test2.action.pos  format json  tag fw.test2.action.log  # tag debug.fw.test2.action.log  </source>  <match fw.test2.action.\*\*>  @type copy  <store>  @type file  path /data/logminor/TD\_LOGS/test2.action/fw.test2.action  time\_slice\_format %Y%m%d  append true  time\_key time\_key  time\_format %Y-%m-%d %H:%M:%S%z  </store>  # <store>  # @type mysql  # host 10.20.10.240  # database fluent\_action\_log  # username fluent  # password fluent  #  # # include\_time\_key yes  # # time\_format %Y-%m-%d %H:%M:%S%z  # # # 2015-06-15 15:53:31  # # # time\_key timekey  # # time\_key time\_key  #  # key\_names time\_key, \_key,action,site,section.id, uid,ippcd,pcid,client.ip,category.no, item.no,item.price,order.no,order.type,order.status, url,url.ref  # sql call sp\_test2\_action\_log\_ins ( ?,?,?,?,?, ?,?,?,?,?, ?,?,?,?,?, ?,?)  #  # # key\_names timekey, \_key, action, site, section.id, uid,ippcd,pcid,client.ip,category.no, item.no,item.price,item.price,order.no,order.type, order.status,url,url.ref  # # sql INSERT INTO shop\_action\_log ( time\_key,tag\_key,action,site,section\_id, uid,ippcd,pcid,client\_ip,category\_no, item\_no,item\_price,order\_no,order\_type, order\_status,url,url\_ref) VALUES (?,?,?,?,?, ?,?,?,?,?, ?,if(?='',0, ?),?,?, ?,?,?)  #  # # key\_names timekey, \_key, url,url.ref  # # sql call sp\_test ( ?,?, ?, ?)  #  # buffer\_type file  # buffer\_path /data/fluent\_buffer/test2/test2\_action.\*.sqlbuf  #  # # flush\_interval 30s  # flush\_interval 10s  # </store>  #  # <store>  # @type elasticsearch  #  # logstash\_format true  #  # # host 211.233.74.68  # # host 127.0.0.1  # # port 9200  #  # host 10.20.10.240  # port 9200  #  # request\_timeout 15s  #  # logstash\_format true  # logstash\_prefix test2\_action  #  # type\_name actionlog  #  # logstash\_dateformat %Y%m%d  # utc\_index true  #  #  # # include\_tag\_key true  # # tag\_key \_key  #  # buffer\_type file  # buffer\_path /data/fluent\_buffer/test2/test\_action.\*.buffer  #  # # flush\_interval 20s # for testing  # flush\_interval 20s  # retry\_limit 7  # retry\_wait 10s  # num\_threads 2  #  # </store>  </match> |

|  |
| --- |
| /\*DDL Information\*/  -------------------  CREATE TABLE `shop\_action\_item\_log` (  `seq` bigint(20) NOT NULL AUTO\_INCREMENT,  `time\_key` datetime NOT NULL DEFAULT '0000-00-00 00:00:00',  `tag\_key` varchar(50) DEFAULT NULL,  `action` varchar(50) DEFAULT NULL,  `site` varchar(50) DEFAULT NULL,  `section\_id` varchar(50) DEFAULT NULL,  `uid` varchar(50) DEFAULT NULL,  `ippcd` varchar(15) DEFAULT NULL,  `pcid` varchar(50) DEFAULT NULL,  `client\_ip` varchar(50) DEFAULT NULL,  `category\_no` varchar(20) DEFAULT NULL,  `item\_no` varchar(30) DEFAULT NULL,  `item\_price` bigint(20) DEFAULT NULL,  `order\_no` varchar(40) DEFAULT NULL,  `order\_type` varchar(20) DEFAULT NULL,  `order\_status` varchar(10) DEFAULT NULL,  `url\_id` bigint(20) DEFAULT NULL,  `url\_id\_ref` bigint(20) DEFAULT NULL,  PRIMARY KEY (`seq`,`time\_key`),  KEY `shop\_action\_item\_log\_idx1` (`time\_key`)  ) ENGINE=MyISAM AUTO\_INCREMENT=817 DEFAULT CHARSET=utf8  /\*!50100 PARTITION BY LIST ( MONTH(time\_key))  (PARTITION p1 VALUES IN (1) ENGINE = MyISAM,  PARTITION p2 VALUES IN (2) ENGINE = MyISAM,  PARTITION p3 VALUES IN (3) ENGINE = MyISAM,  PARTITION p4 VALUES IN (4) ENGINE = MyISAM,  PARTITION p5 VALUES IN (5) ENGINE = MyISAM,  PARTITION p6 VALUES IN (6) ENGINE = MyISAM,  PARTITION p7 VALUES IN (7) ENGINE = MyISAM,  PARTITION p8 VALUES IN (8) ENGINE = MyISAM,  PARTITION p9 VALUES IN (9) ENGINE = MyISAM,  PARTITION p10 VALUES IN (10) ENGINE = MyISAM,  PARTITION p11 VALUES IN (11) ENGINE = MyISAM,  PARTITION p12 VALUES IN (12) ENGINE = MyISAM) \*/ |

|  |
| --- |
| CREATE TABLE `shop\_action\_url\_log` (  `url\_id` bigint(20) NOT NULL AUTO\_INCREMENT,  `url` varchar(250) NOT NULL,  `url\_parm` varchar(250) NOT NULL DEFAULT '',  `action` varchar(100) DEFAULT NULL,  `reg\_date` datetime DEFAULT NULL,  `uid` bigint(20) DEFAULT NULL,  PRIMARY KEY (`url\_id`),  UNIQUE KEY `shop\_action\_url\_uk` (`url`,`url\_parm`)  ) ENGINE=InnoDB AUTO\_INCREMENT=157 DEFAULT CHARSET=utf8 |

|  |
| --- |
| /\*Stored Proc: sp\_action\_log\_ins\*/  ----------------------------------  Create Procedure:  -----------------  CREATE DEFINER=`dbadmin`@`10.20.4.%` PROCEDURE `**sp\_action\_log\_ins**`(IN v\_time\_key TIMESTAMP, IN v\_tag\_key VARCHAR(100),IN v\_action VARCHAR(100),  IN v\_site VARCHAR(100),IN v\_section\_id VARCHAR(50),  IN v\_uid VARCHAR(100), IN v\_ippcd VARCHAR(100),IN v\_pcid VARCHAR(100),IN v\_client\_ip VARCHAR(100),  IN v\_category\_no VARCHAR(100), IN v\_item\_no VARCHAR(100),IN v\_item\_price VARCHAR(100),  IN v\_order\_no VARCHAR(100),IN v\_order\_type VARCHAR(100),IN v\_order\_status VARCHAR(100),  IN v\_url VARCHAR(250),IN v\_url\_ref VARCHAR(250))  COMMENT 'Proc INSERT shop\_action\_item\_log shop\_action\_url\_log '  BEGIN  DECLARE tmp\_url\_id BIGINT(20) DEFAULT 0;  DECLARE tmp\_url\_id\_ref BIGINT(20) DEFAULT 0;    DECLARE m\_done INT DEFAULT 0;    -- // START url-----------------------------------------------  **-- 테이블에 값을 입력하고, 키값을 받아오는 부분 (매우중요)**  IF LENGTH(v\_url) > 10 THEN  INSERT INTO `shop\_action\_url\_log` ( url, url\_parm, `action` )  VALUES ( SUBSTRING\_INDEX(v\_url, '?', 1), IF( LOCATE('?', v\_url), SUBSTRING\_INDEX(v\_url, '?', -1), '' ), v\_action )  ON DUPLICATE KEY UPDATE  uid = IF(@tmp\_uid := url\_id, url\_id, url\_id),  reg\_date = now();    SET tmp\_url\_id := IF( LAST\_INSERT\_ID(), LAST\_INSERT\_ID(), @tmp\_uid);  ELSE  SET tmp\_url\_id := 0;  END IF;      -- // START url\_ref-----------------------------------------------    IF LENGTH(v\_url\_ref) > 10 THEN    INSERT INTO `shop\_action\_url\_log` ( url, url\_parm, `action` )  VALUES ( SUBSTRING\_INDEX(v\_url\_ref, '?', 1), IF( LOCATE('?', v\_url\_ref), SUBSTRING\_INDEX(v\_url\_ref, '?', -1), '' ), v\_action )  ON DUPLICATE KEY UPDATE  uid = IF(@tmp\_uid := url\_id, url\_id, url\_id),  reg\_date = NOW();    SET tmp\_url\_id\_ref := IF( LAST\_INSERT\_ID(), LAST\_INSERT\_ID(), @tmp\_uid);  ELSE  SET tmp\_url\_id\_ref := 0;  END IF;    -- // shop\_action\_url\_log -----------------------------------------------    INSERT INTO `shop\_action\_item\_log` ( time\_key, tag\_key, ACTION, site, section\_id, uid,ippcd, pcid, client\_ip,  category\_no, item\_no, item\_price, order\_no, order\_type, order\_status, url\_id, url\_id\_ref)  VALUES ( FROM\_UNIXTIME( UNIX\_TIMESTAMP( v\_time\_key)), v\_tag\_key, v\_action, v\_site, v\_section\_id, v\_uid, v\_ippcd, v\_pcid, v\_client\_ip,  v\_category\_no, v\_item\_no, v\_item\_price, v\_order\_no, v\_order\_type, v\_order\_status, tmp\_url\_id, tmp\_url\_id\_ref);        -- SELECT LAST\_INSERT\_ID() AS log\_insert\_id;  END  sql\_mode:  --------- |

서버 목록