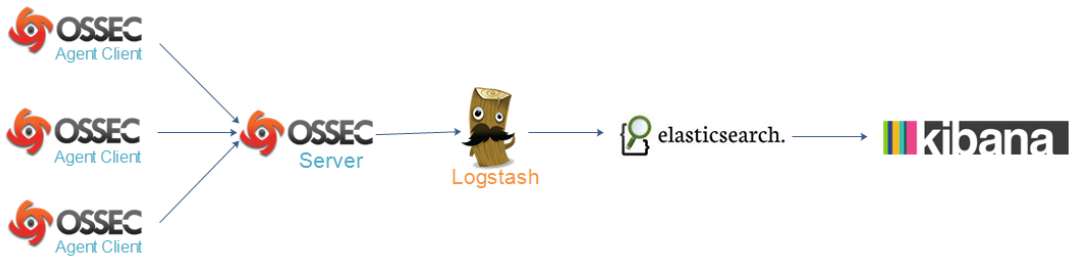
Ossec IDS+Logash+Elasticsearch+Kibana　安装部署

环境

类型	操作系统	IP	软件包
服务端	Centos 6.5 X64	10.10.51.50	ossec-hids-2.8.2 、 JDK1.8 、 Logstash-1.5.2 、elasticsearch-1.4.4、Kibana-4.0.2
客户端	Centos 6.5 X64	10.10.51.51	ossec-hids-2.8.2

注：Logash、Elasticsearch、Kibana 运行需要 JDK

Ossec logstash elasticsearch kibana 流程图



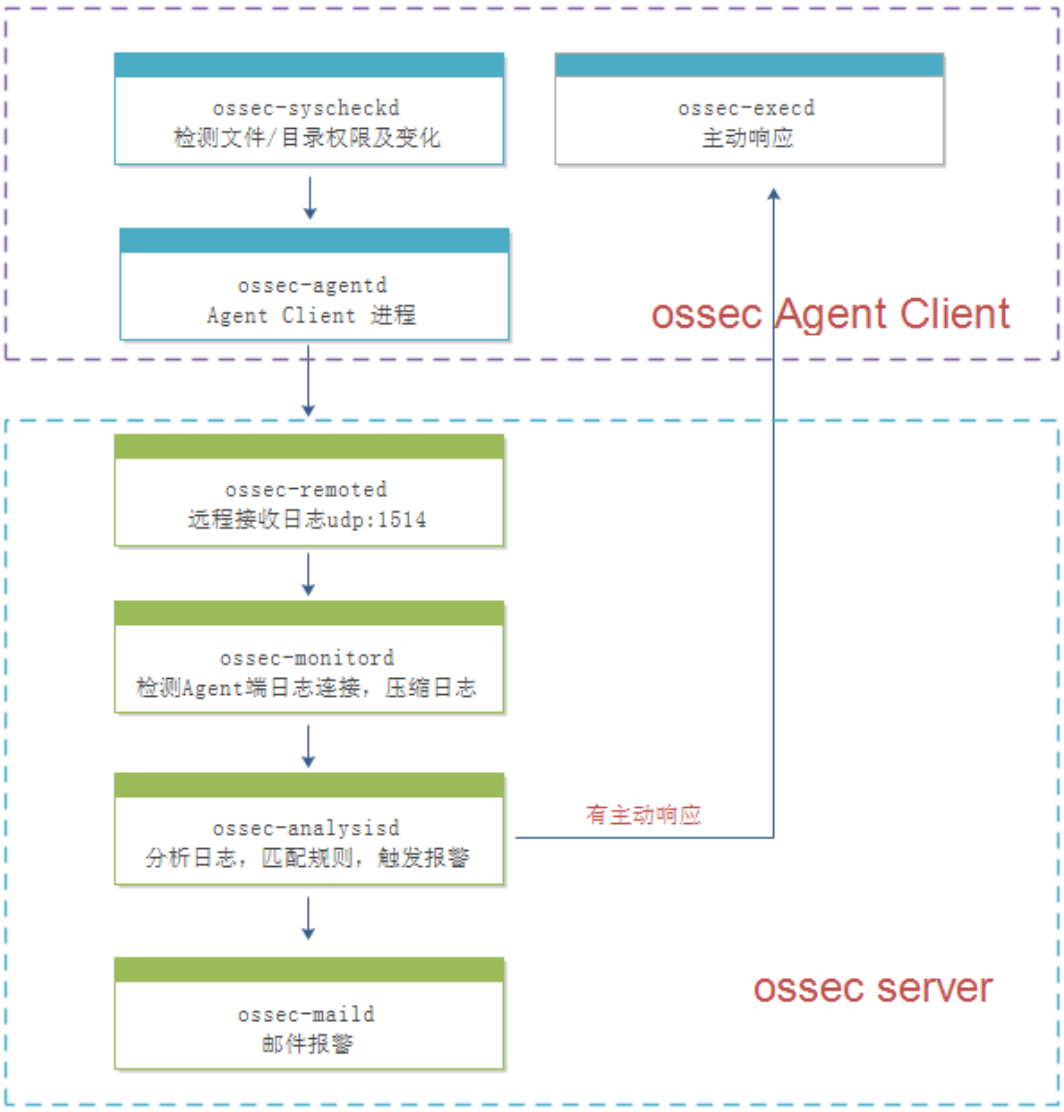
Ossec 介绍

OSSEC 是一款开源的多平台的入侵检测系统，可以运行于 Windows, Linux, OpenBSD/FreeBSD, 以及 MacOS 等操作系统中。
官方网站: http://www.ossec.net

Ossec 四大功能

- 文件目录检测
- 日志分析
- 入侵检测
- 自动响应

Ossec 逻辑图



Ossec 常用进程说明

ossec-maild	#邮件通知
ossec-execd	#主动响应
ossec-analysisd	#分析日志，匹配规则，触发报警
ossec-logcollector	#检测 ossec 配置文件
ossec-remoted	#远程接收日志，开放 udp:1514 端口，给 Agent 使用
ossec-syscheckd	#检测文件/目录权限及变化
ossec-monitord	#检测 agent 端日志连接，压缩日志

Ossec server 安装

#tar zxvf ossec-hids-2.8.2.tar.gz
#cd ossec-hids-2.8.2
#./install.sh

```
[root@localhost ossec-hids-2.8.2]# ./install.sh

 ** Para instala??o em português, escolha [br].
 ** 要使用中文进行安装，请选择 [cn].
 ** Fur eine deutsche Installation wohlen Sie [de].
 ** Γ ι α  ε γ κ α τ?σ τ α σ η  σ τ α  Ε λ λ η ν ι κ?,  ε π ι λ?ξ τ ε  [el].
 ** For installation in English, choose [en].
 ** Para instalar en Espa?ol , eliga [es].
 ** Pour une installation en fran?ais, choisissez [fr]
 ** A Magyar nyelv? telepítéshez válassza [hu].
 ** Per l'installazione in Italiano, scegli [it].
 ** 日本語でインストールします．選択して下さい．[jp].
 ** Voor installatie in het Nederlands, kies [nl].
 ** Aby instalowa? w j?zyku Polskim, wybierz [pl].
 ** Д л я  и н с т р у к ц и й  п о  у с т а н о в к е  н а  р у с с к о м ,  в в е д и т е  [ru].
 ** Za instalaciju na srpskom, izaberi [sr].
 ** Türk?e kurulum i?in se?in [tr].
 (en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]: cn
```

选择安装语言

```
OSSEC HIDS v2.8 安装脚本 - http://www.ossec.net

您将开始 OSSEC HIDS 的安装.
请确认在您的机器上已经正确安装了 C 编译器.
如果您有任何疑问或建议,请给 dcid@ossec.net (或 daniel.cid@gmail.com) 发邮件.

 - 系统类型: Linux localhost.localdomain 2.6.32-504.23.4.el6.x86_64
 - 用户: root
 - 主机: localhost.localdomain


 -- 按 ENTER 继续或 Ctrl-C 退出. --


1- 您希望哪一种安装 (server, agent, local or help)? server
```

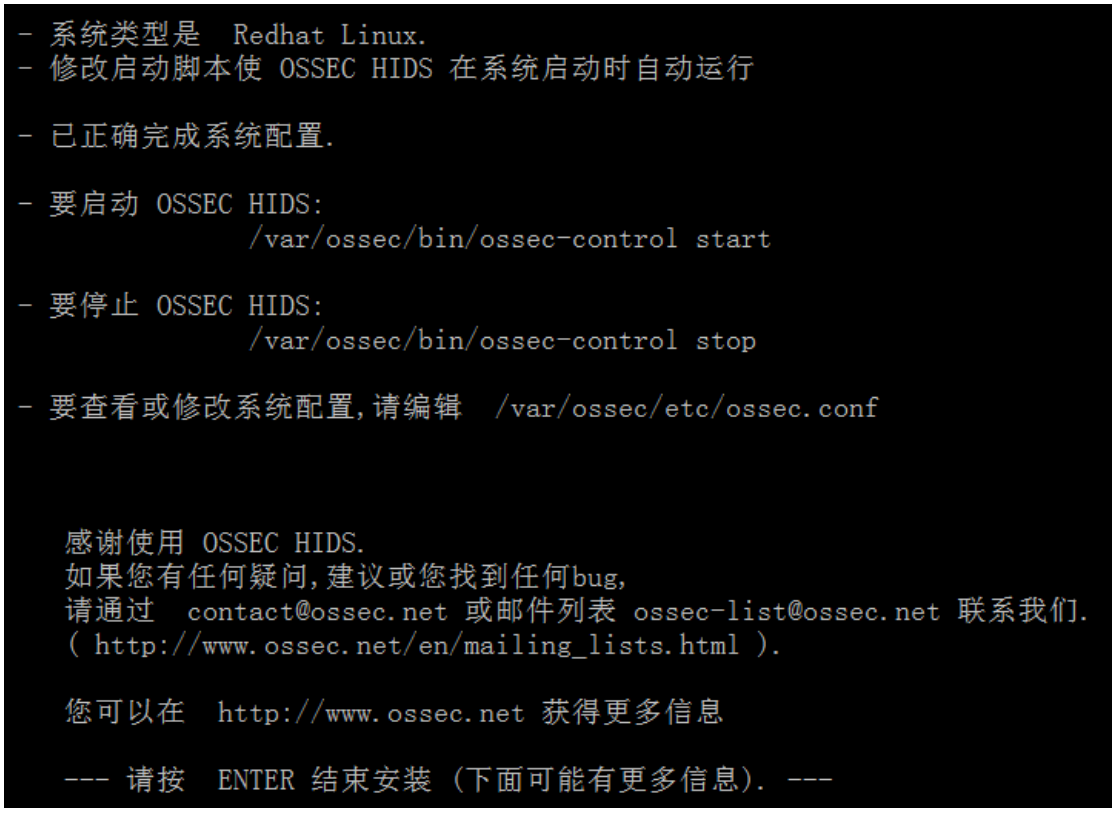
选择安装类型

注: server 为服务端
agent 为代理端，可向 server 端注册
local 为本地端，如果只有一台服务器，可以选择 local 自己监控自己

```
1- 您希望哪一种安装 (server, agent, local or help)? server

  - 选择了 Server 类型的安装.

2- 正在初始化安装环境.

 - 请选择 OSSEC HIDS 的安装路径 [/var/ossec]:

    - OSSEC HIDS 将安装在  /var/ossec .

3- 正在配置 OSSEC HIDS.

  3.1- 您希望收到e-mail告警吗? (y/n) [y]: y
   - 请输入您的 e-mail 地址? ossec@163.com

   - 我们找到您的 SMTP 服务器为: 163mx01.mxmail.netease.com.
   - 您希望使用它吗? (y/n) [y]: y

   --- 使用 SMTP 服务器:  163mx01.mxmail.netease.com.

  3.2- 您希望运行系统完整性检测模块吗? (y/n) [y]: y

   - 系统完整性检测模块将被部署.

  3.3- 您希望运行 rootkit检测吗? (y/n) [y]: y

   - rootkit检测将被部署.

  3.4- 关联响应允许您在分析已接收事件的基础上执行一个
       已定义的命令.
       例如,你可以阻止某个IP地址的访问或禁止某个用户的访问权限.
       更多的信息,您可以访问:
       http://www.ossec.net/en/manual.html#active-response
   - 您希望开启联动(active response)功能吗? (y/n) [y]: y
```

```
 - 默认情况下，我们开启了主机拒绝和防火墙拒绝两种响应.
   第一种情况将添加一个主机到 /etc/hosts.deny.
   第二种情况将在iptables(linux)或ipfilter(Solaris,
   FreeBSD 或 NetBSD) 中拒绝该主机的访问.
 - 该功能可以用以阻止 SSHD 暴力攻击，端口扫描和其他
   一些形式的攻击. 同样你也可以将他们添加到其他地方,
   例如将他们添加为 snort 的事件.

 - 您希望开启防火墙联动(firewall-drop)功能吗? (y/n) [y]: y

   - 防火墙联动(firewall-drop)当事件级别 >= 6 时被启动

 - 联动功能默认的白名单是:
    - 10.10.15.2
    - 114.114.114.114

 - 您希望添加更多的IP到白名单吗? (y/n)? [n]: y
 - 请输入IP (用空格进行分隔):

3.5- 您希望接收远程机器syslog吗 (port 514 udp)? (y/n) [y]: y

 - 远程机器syslog将被接收.

3.6- 设置配置文件以分析一下日志:
  -- /var/log/messages
  -- /var/log/secure
  -- /var/log/maillog
  -- /var/log/nginx/access.log (apache log)
  -- /var/log/nginx/error.log (apache log)


-如果你希望监控其他文件，只需要在配置文件ossec.conf中
 添加新的一项.
 任何关于配置的疑问您都可以在 http://www.ossec.net 找到答案.


 --- 按 ENTER 以继续 ---
```

设置相关功能



安装完成

Ossec Server 启动

#/etc/init.d/ossec start

Ossec 目录介绍

#tree /opt/ossec/

/var/ossec/

```
├─── active-response        #ossec 自动响应脚本目录
├─── agentless              #代理目录，主要用于不能安装 client 设置，如交换机
├─── bin                    #ossec 程序执行目录
├─── etc                    #ossec 配置目录
├─── logs                   #ossec 日志目录
├─── queue                  #ossec 队列目录，用于系统检测，文件对比
├─── rules                  #ossec 规则目录
├─── stats                  #ossec 统计目录
├─── tmp                    #ossec 临时目录
└─── var                    #ossec  pid 目录
```

Ossec Client 客户端安装

#tar zxvf ossec-hids-2.8.2.tar.gz
#cd ossec-hids-2.8.2
#./install.sh

```
[root@localhost ossec-hids-2.8.2]# ./install.sh

 ** Para instala??o em português, escolha [br].
 ** 要使用中文进行安装, 请选择 [cn].
 ** Fur eine deutsche Installation wohlen Sie [de].
 ** Γ ι α  ε γ κ α τ?σ τ α σ η  σ τ α  Ε λ λ η ν ι κ?, ε π ι λ?ξ τ ε  [el].
 ** For installation in English, choose [en].
 ** Para instalar en Espa?ol , eliga [es].
 ** Pour une installation en fran?ais, choisissez [fr]
 ** A Magyar nyelv? telepítéshez válassza [hu].
 ** Per l'installazione in Italiano, scegli [it].
 ** 日本語でインストールします. 選択して下さい. [jp].
 ** Voor installatie in het Nederlands, kies [nl].
 ** Aby instalowa? w j?zyku Polskim, wybierz [pl].
 ** Д л я  и н с т р у к ц и й  п о  у с т а н о в к е  н а  р у с с к о м ,  в в е д и т е  [ru].
 ** Za instalaciju na srpskom, izaberi [sr].
 ** Türk?e kurulum i?in se?in [tr].
 (en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]: cn
```

选择安装语言

```
OSSEC HIDS v2.8 安装脚本 - http://www.ossec.net

您将开始 OSSEC HIDS 的安装.
请确认在您的机器上已经正确安装了 C 编译器.
如果您有任何疑问或建议,请给 dcid@ossec.net (或 daniel.cid@gmail.com) 发邮件.

 - 系统类型: Linux web-10-10-51-51 2.6.32-504.23.4.el6.x86_64
 - 用户: root
 - 主机: web-10-10-51-51


 -- 按 ENTER 继续或 Ctrl-C 退出. --


1- 您希望哪一种安装 (server, agent, local or help)? agent
```

选择安装类型，agent 客户端

```
1- 您希望哪一种安装 (server, agent, local or help)? agent

 - 选择了 Agent(client) 类型的安装.

2- 正在初始化安装环境.

 - 请选择 OSSEC HIDS 的安装路径 [/var/ossec]:

   - OSSEC HIDS 将安装在  /var/ossec .

3- 正在配置 OSSEC HIDS.

 3.1- 请输入 OSSEC HIDS 服务器的IP地址或主机名: 10.10.51.50

  - 添加服务器IP  10.10.51.50

 3.2- 您希望运行系统完整性检测模块吗? (y/n) [y]: y

  - 系统完整性检测模块将被部署.

 3.3- 您希望运行 rootkit检测吗? (y/n) [y]: y

  - rootkit检测将被部署.

 3.4 - 您希望开启联动(active response)功能吗? (y/n) [y]: y


 3.5- 设置配置文件以分析一下日志:
   -- /var/log/messages
   -- /var/log/secure
   -- /var/log/maillog
   -- /var/log/nginx/access.log (apache log)
   -- /var/log/nginx/error.log (apache log)


-如果你希望监控其他文件, 只需要在配置文件ossec.conf中
```

设置相关功能

```
- 系统类型是  Redhat Linux.
- 修改启动脚本使 OSSEC HIDS 在系统启动时自动运行

- 已正确完成系统配置.

- 要启动 OSSEC HIDS:
              /var/ossec/bin/ossec-control start

- 要停止 OSSEC HIDS:
              /var/ossec/bin/ossec-control stop

- 要查看或修改系统配置,请编辑  /var/ossec/etc/ossec.conf



   感谢使用 OSSEC HIDS.
   如果您有任何疑问,建议或您找到任何bug,
   请通过  contact@ossec.net 或邮件列表 ossec-list@ossec.net 联系我们.
   ( http://www.ossec.net/en/mailing_lists.html ).

   您可以在  http://www.ossec.net 获得更多信息

   --- 请按  ENTER 结束安装 (下面可能有更多信息). ---


- 您必须首先将该代理添加到服务器端以使他们能够相互通信.
  这样做了以后,您可以运行'manage_agents'工具导入
  服务器端产生的认证密匙.
  /var/ossec/bin/manage_agents

  详细信息请参考:
  http://www.ossec.net/en/manual.html#ma
```

安装完成

Ossec client 启动

/etc/init.d/ossec start

Ossec Client 认证注册

Ossec Server 端，生成客户端密钥

[root@localhost bin]# /var/ossec/bin/manage_agents

```
****************************************
* OSSEC HIDS v2.8 Agent manager.        *
* The following options are available: *
****************************************
    (A)dd an agent (A).                                  #添加客户端
    (E)xtract key for an agent (E).                      #提取客户端密钥
    (L)ist already added agents (L).                     #查看已注册认证客户端
    (R)emove an agent (R).                               #移除客户端
    (Q)uit.                                              #退出
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
    * A name for the new agent: web-10-10-51-51          #客户端名称
    * The IP Address of the new agent: 10.10.51.51       #客户端 IP 地址
    * An ID for the new agent[001]:                      #ID 号，默认即可
Agent information:
    ID:001
    Name:web-10-10-51-51
    IP Address:10.10.51.51

Confirm adding it?(y/n): y                               #确认是否添加
Agent added.
```

提取客户端密钥

```
****************************************
* OSSEC HIDS v2.8 Agent manager.         *
* The following options are available: *
****************************************
    (A)dd an agent (A).
    (E)xtract key for an agent (E).
    (L)ist already added agents (L).
    (R)emove an agent (R).
    (Q)uit.
Choose your action: A,E,L,R or Q: E                    #提取客户端密钥

Available agents:
    ID: 001, Name: web-10-10-51-51, IP: 10.10.51.51
Provide the ID of the agent to extract the key (or '\q' to quit): 001       #输入客户端 ID

Agent key information for '001' is:                    #客户端密钥
MDAxIHdlYi0xMC0xMC01MS01MSAxMC4xMC41MS41MSBkZDNmZWExOTBlMGNjMmJjYzY2YjYz
OGZiYzEwMTc2YmI1MDljNGViZGVmNDA3YmE5Zjg2ZTE3MmIzNTQyNjIz

** Press ENTER to return to the main menu.
```

ossec Client 端，导入密钥

```
[root@web-10-10-51-51 bin]# /var/ossec/bin/manage_agents

****************************************
* OSSEC HIDS v2.8 Agent manager.         *
* The following options are available: *
****************************************
    (I)mport key from the server (I).
    (Q)uit.
Choose your action: I or Q: I                          #导入密钥

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit):                       #输入密钥，ossec server 端生成时的密钥
MDAxIHdlYi0xMC0xMC01MS01MSAxMC4xMC41MS41MSBkZDNmZWExOTBlMGNjMmJjYzY2YjYz
OGZiYzEwMTc2YmI1MDljNGViZGVmNDA3YmE5Zjg2ZTE3MmIzNTQyNjIz

Agent information:
    ID:001
```

Name:web-10-10-51-51
IP Address:10.10.51.51

Confirm adding it?(y/n): y
Added.
** Press ENTER to return to the main menu.

导入成功后，会在 ossec 目录后成 client.keys 文件
#cat /var/ossec/etc/client.keys
001 web-10-10-51-51 10.10.51.51
dd3fea190e0cc2bcc66b638fbc10176bb509c4ebdef407ba9f86e172b3542623

查看 agent client 端是否激活
[root@ossec-server-10-10-51-50]# /var/ossec/bin/agent_control -l
OSSEC HIDS agent_control. List of available agents:
ID: 000, Name: ossec-server-10-10-51-50 (server), IP: 127.0.0.1, Active/Local
ID: 002, Name: web-10-10-51-51, IP: 10.10.51.51, Active

Ossec 配置说明

Ossec 配置文件
/var/ossec/etc/ossec.conf

配置邮件通知

```
<global>
    <email_notification>yes</email_notification>      #是否接收邮件通知
    <email_to>info@163.com</email_to>                 #收件人地址
    <smtp_server>smtp.163.com.</smtp_server>          #发邮件 smtp 地址
    <email_from>send@163.com</email_from>             #发件人地址
</global>
```

加载自定义规则

```
<rules>
    <include>test_rules_config.xml</include>     #加载 test_rules_config 规则
</rules>
```

文件目录检测

```
<syscheck>
    <!-- Frequency that syscheck is executed - default to every 22 hours -->
    <frequency>79200</frequency>                                    #检测时间

    <!-- Directories to check    (perform all possible verifications) -->
    <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
    <directories check_all="yes">/bin,/sbin</directories>       #检测目录
    <directories check_all="yes">/opt/web/upload</directories>

    <!-- Files/directories to ignore -->
    <ignore>/etc/mtab</ignore>                      #忽略检测目录
</syscheck>
```

注: check_all=”yes”　检测以下所有类型

检测类型有:

```
check_sum=“yes”                #MD5 和  SHA1
check_sha1sum =“yes”           #SHA1
check_md5sum=“yes”             #MD5
check_size =“yes”              #文件大小
check_owner =“yes”             #文件所有者
check_group=“yes”              #文件组
check_pem=“yes”                #文件权限
restrict=“string”               #文件字符串，文件内容中包含文件名的字符串限制检查

type="sregex"                  #支持正则
realtime="yes"                 #启用实时监控
report_changes="yes"           #发送文件变化比较报告
```

入侵检测

```
<rootcheck>
  <rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files> #后门，蠕虫，嗅探检测
  <rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>   #木马检测
  <system_audit>/var/ossec/etc/shared/system_audit_rcl.txt</system_audit>
</rootcheck>
```

白名单

```
<global>
    <white_list>127.0.0.1</white_list>
    <white_list>8.8.8.8</white_list>
    <white_list>10.10.51.50</white_list> #白名单地址，ossec 不会白名单地址进行主动响应
</global>
```

允许远程日志分析

```
<remote>
    <connection>syslog</connection>              #系统日志
</remote>
<remote>
    <connection>secure</connection>              #安全日志
</remote>
```

记录日志/邮件通知

```
<alerts>
    <log_alert_level>1</log_alert_level>          #记录等级大于 1 的报警日志
    <email_alert_level>7</email_alert_level>      #等级大于 7，邮件通知
</alerts>
```

注：ossec 等级分为 0-15，0 等级最低，15 最高。

定义脚本命令

```
<command>
    <name>firewall-drop</name>                    #名称
    <executable>firewall-drop.sh</executable>     #脚本名称
    <expect>srcip</expect>                        #脚本参数
    <timeout_allowed>yes</timeout_allowed>        #是否允许超时
</command>
```

主动响应

```
<active-response>
    <command>firewall-drop</command>          #命令名称与上面定义脚本名称相匹配
    <location>local</location>                #在本地执行
    <level>6</level>                          #等级
    <timeout>600</timeout>                    #超时时间
</active-response>
```

日志监控

```
<localfile>
    <log_format>syslog</log_format>           #日志格式
    <location>/var/log/messages</location>    #日志路径
</localfile>
```

Ossec 配置实例

监控文件/目录
修改 ossec.conf 配置文件，加入以下内容：

```
<syscheck>
    <directories check_all="yes">/opt/web</directories>      #检测目录
    <ignore>/var/web/upload</ignore>                          #忽略 upload 目录检测
    <ignore>/var/web/config.conf</ignore>                     #忽略 config.conf 文件检测
</syscheck>
```

监控 web 日志
修改 ossec.conf 配置文件，加入以下内容：

```
  <localfile>
    <log_format>apache</log_format>                 #日志格式
    <location>/var/log/nginx/error.log</location>    #web 日志路径
  </localfile>
```

入侵检测
修改 ossec.conf 配置文件<rootcheck>标签定义的规则文件，达到入侵检测的目的。
比如某种后门会在/tmp 目录下生成 mcrootkit 文件，在/var/ossec/etc/shared/rootkit_files.txt 文件中添加如下内容：

```
tmp/mcrootkit     ! Bash door ::/rootkits/bashdoor.php
```

邮件通知信息

```
OSSEC HIDS Notification.
2015 Jul 07 18:19:14
Received From: (web-10-10-51-51) 10.10.51.51->rootcheck
Rule: 510 fired (level 7) -> "Host-based anomaly detection event (rootcheck)."
Portion of the log(s):
Rootkit 'Bash' detected by the presence of file '/tmp/secrootkit'.
--END OF NOTIFICATION
```

自动响应
添加 ddos_rules.xml 文件到 ossec.conf 配置文件中

```
<rules>
    <include> ddos_rules.xml </include>
</rules>
```

建立防 CC 攻击规则

```
# vi /var/ossec/rules/ddos_rules.xml
  <rule id="31177" level="3">                          #定义 rule id
    <if_sid>31108</if_sid>                             #判断 rule id 31108
    <url>^/*.php</url>                                 #匹配 URL 地址中包含任何 php 文件
    <description>CC ATTACKS URL </description>         #描述
  </rule>

<rule id="31178" level="10" frequency="10" timeframe="60">
<if_matched_sid>31177</if_matched_sid>
    <same_source_ip />
    <description>CC ATTACKS</description>
    <group>DDOS</group>
  </rule>
```

说明：

60 秒内同一 IP 访问 php 文件超过 10 次，触发脚本

匹配 urle id 为 31108 的日志中 URL 包含任何 php 文件

关于 rule id 31108 规则详细定义，请查看 web_rules.xml 文件。

```
  <rule id="31108" level="0">
    <if_sid>31100</if_sid>
    <id>^2|^3</id>
    <compiled_rule>is_simple_http_request</compiled_rule>
    <description>Ignored URLs (simple queries).</description>
   </rule>
```

说明：rule id 31108 是匹配 web 日志 2x,3x 访问代码。有效过滤了 404，403 等错误页面

配置自动响应

在 ossec.conf 配置文件中，添加如下内容：

```
<command>
    <name>firewall-drop</name>                    #命令名称
    <executable>firewall-drop.sh</executable>     #执行脚本
    <expect>srcip</expect>                        #脚本参数，客户端 IP
    <timeout_allowed>yes</timeout_allowed>        #允许超时
  </command>
<active-response>
    <command>firewall-drop</command>              #自动响应命令名称，上面定义
    <location>local</location>                    #脚本执行位置，local 表示 agent 端
    <rules_id>31178</rules_id>                    #触发 rule id
    <timeout>600</timeout>                        #超时时间
</active-response>
```

自定义规则
在日志中过滤字符串，比如日志中出现 admin_backdoor，触发报警

添加 test_rules.xml 文件到 ossec.conf 配置文件中

```
<rules>
    <include> test_rules.xml </include>
</rules>
```

创建过滤规则

```
#vi /var/ossec/rules/test_rules.xml
<group name="localtest,">
<rule id="7777" level="7">
    <decoded_as>admin_backdoor</decoded_as>                    #decode 名称
    <description>admin_backdoor access</description>
  </rule>
</group>
```

配置 decoder.xml 文件

```
# vi /var/ossec/etc/decoder.xml
<decoder name="admin_backdoor">                #decoder 名称，与 test_rules.xml 名称匹配
    <prematch>^admin_backdoor</prematch>    #匹配字符串 admin_backdoor
</decoder>
```

报警信息:

```
[root@ossec-server-10-10-51-50 /var/ossec]# ./bin/ossec-logtest
2015/07/07 19:48:20 ossec-testrule: INFO: Reading local decoder file.
2015/07/07 19:48:20 ossec-testrule: INFO: Started (pid: 16189).
ossec-testrule: Type one log per line.

admin_backdoor                                  #输入字符串

**Phase 1: Completed pre-decoding.
        full event: 'admin_backdoor'
        hostname: 'ossec-server-10-10-51-50'
        program_name: '(null)'
        log: 'admin_backdoor'

**Phase 2: Completed decoding.
        decoder: 'admin_backdoor'

**Phase 3: Completed filtering (rules).
        Rule id: '7777'                         #匹配到 rule id 8888
        Level: '7'
        Description: 'admin_backdoor access'    #描述，上面定义好的
**Alert to be generated.
```

JDK 安装

#yum install java-1.8.0-openjdk

Elasticsearch 安装

#tar zxvf elasticsearch-1.4.4.tar.gz -C /opt
配置
#vi /opt/elasticsearch-1.4.4/conf/elasticsearch.yml
加入下面内容:
http.cors.enabled: true
http.cors.allow-origin: "*"

注: 默认端口:9200

Elasticsearch 启动

#/opt/elasticsearch-1.4.4/bin/elasticsearch -Xmx2g -Xms2g -Des.index.storage.type=memory –d
注: -Xmx2g 为最小内存和最大内存
-d 后台运行

创建 Elasticsearch ossec 日志模板

```
# curl    -XPUT http://127.0.0.1:9200/_template/template_ossec -d '
{
   "template" : "osseclog-*",
   "settings" : {
      "index.refresh_interval" : "5s"
   },
   "mappings" : {
      "_default_" : {
          "_all" : {"enabled" : true},
          "dynamic_templates" : [ {
            "string_fields" : {
              "match" : "*",
              "match_mapping_type" : "string",
              "mapping" : {
                "type" : "string", "index" : "analyzed", "omit_norms" : true,
                  "fields" : {
                    "raw" : { "type": "string", "index" : "not_analyzed", "ignore_above" : 256,
"doc_values": true }
                  }
              }
            }
          } ],
          "properties" : {
            "@version": { "type": "string", "index": "not_analyzed" },
            "@timestamp": { "type": "date", "index": "not_analyzed", "doc_values": true, "format":
"dateOptionalTime" },
            "geoip"    : {
              "type" : "object",
                "dynamic": true,
                "path": "full",
                "properties" : {
                  "location" : { "type" : "geo_point" }
                }
            }
          }
      }
   }
}'
```

Logstash 安装

#tar zxvf logstash-1.5.2.tar.gz –C /opt

Logstash 配置

添加 ossec 报警日志 logstash 配置

#mkdir /opt/logstash-1.4.2/etc

#vi /opt/logstash-1.4.2/etc/ossec.conf

```
# original idea by Joshua Garnett
input {
  file {
    type => "ossec"
    path => "/var/ossec/logs/alerts/alerts.log"
    codec => multiline {
      pattern => "^\*\*"
      negate => true
      what => "previous"
    }
  }
}
filter {
  if [type] == "ossec" {
# Parse the header of the alert
    grok {
      match => ["message", "(?m)\*\*
Alert %{DATA:timestamp_seconds}:%{SPACE}%{WORD}?%{SPACE}\- %{DATA:ossec_group}\n%{YE
AR} %{SYSLOGTIMESTAMP:syslog_timestamp} \(%{DATA:reporting_host}\) %{IP:reporting_ip}\-
\>%{DATA:reporting_source}\nRule: %{NONNEGINT:rule_number}
\(level %{NONNEGINT:severity}\) \-\> '%{DATA:signature}'\n%{GREEDYDATA:remaining_message}"]
      match => ["message", "(?m)\*\*
Alert %{DATA:timestamp_seconds}:%{SPACE}%{WORD}?%{SPACE}\- %{DATA:ossec_group}\n%{YE
AR} %{SYSLOGTIMESTAMP:syslog_timestamp} %{DATA:reporting_host}\-
\>%{DATA:reporting_source}\nRule: %{NONNEGINT:rule_number}
\(level %{NONNEGINT:severity}\) \-\> '%{DATA:signature}'\n%{GREEDYDATA:remaining_message}"]
    }
    # Attempt to parse additional data from the alert
    grok {
      match => ["remaining_message", "(?m)(Src IP: %{IP:src_ip}%{SPACE})?(Src
Port: %{NONNEGINT:src_port}%{SPACE})?(Dst IP: %{IP:dst_ip}%{SPACE})?(Dst
Port: %{NONNEGINT:dst_port}%{SPACE})?(User: %{USER:acct}%{SPACE})?%{GREEDYDATA:real_m
essage}"]
```

```
        }
        geoip {
            source => "src_ip"
        }
        mutate {
            convert          => [ "severity", "integer"]
            replace          => [ "@message", "%{real_message}" ]
            replace          => [ "@fields.hostname", "%{reporting_host}"]
            add_field        => [ "@fields.product", "ossec"]
            add_field        => [ "raw_message", "%{message}"]
            add_field        => [ "ossec_server", "%{host}"]
            remove_field  =>  [  "type",  "syslog_program",  "syslog_timestamp",  "reporting_host",
"message", "timestamp_seconds", "real_message", "remaining_message", "path", "host", "tags"]
        }
    }
}
output {
            stdout { codec => rubydebug }
            elasticsearch_http {
                        host => "127.0.0.1"
                        port => "9200"
            index => "osseclog-%{+YYYY.MM.dd}"
            }
}
```

Logstash 启动

```
# /opt/logstash-1.4.2/bin/logstash -f /opt/logstash-1.4.2/etc/ossec.conf > /dev/null 2>&1 &
```

Kibana 安装

```
#tar zxvf kibana-4.0.2-linux-x64.tar.gz -C /opt
```

配置

```
#vi /opt/logash/kibana-4.0.2-linux-x64/config/kibana.yml
```

添加 elasticsearch 地址，添加即可。

elasticsearch_url: http://localhost:19200

Kibana 启动

```
#/opt/logash/kibana-4.0.2-linux-x64/bin/kibana -p 25601 > /dev/null 2>&1 &
```

注: -p 指定端口，默认端口 5601

Kibana 日志分析展示