BIG-IP ASM相关配置

1. 实验漏洞网站DVWA搭建（可选）

该网站是可选配置项，主要用于测试使用。在实际部署中对应为客户的实际后端服务。

1. PHP环境安装

首先我们在centos 7下使用LAMP来快速安装Apache+MySQL+PHP环境。执行 wget -c http://soft.vpser.net/lnmp/lnmp1.4.tar.gz && tar zxf lnmp1.4.tar.gz && cd lnmp1.4 && ./install.sh lamp 命令，然后除了Mysql密码设置外，一路回车即可。

1. 配置DVWA
2. 在centos下使用命令wget https://github.com/ethicalhack3r/DVWA/archive/master.zip 下载DVWA。
3. 将DVWA文件夹放入 /home/wwwroot/default/ 内。
4. 进入 /home/wwwroot/default/DVWA/config，使用 cp config.inc.php.dist config.inc.php 命令复制一份配置文件。
5. 使用 vim config.inc.php 命令编辑配置文件，将 $\_DVWA[ ‘db\_user’ ] 字段修改为 ‘root’ ，$\_DVWA[ ‘db\_password’ ] 字段修改为安装LAMP时设置的Mysql的密码。（如果没设置Mysql密码，可以在LAMP安装成功的提示中看到默认密码）。
6. 登录进DVWA界面，在DVWA Security界面中将Security Level从Impossible 改为 Low 。
7. 常见问题
8. DVWA默认登录账号密码为 admin/password 。
9. 在setup.php界面如果有红字 PHP function allow\_url\_include: Disabled ，使用 vim /usr/local/php/etc/php.inc 命令，将 allow\_url\_include = Off 改为 On，然后使用service httpd restart重启Apache。
10. 遇到下面问题：

[User: root] Writable folder /home/wwwroot/default/DVWA/hackable/uploads/: No  
[User: root] Writable file /home/wwwroot/default/DVWA/external/phpids/0.6/lib/IDS/tmp/phpids\_log.txt: No

[User: root] Writable folder /home/wwwroot/default/DVWA/config: No

可以通过下面命令解决：

chmod 777 /home/wwwroot/default/DVWA/hackable/uploads

chmod 777 /home/wwwroot/default/DVWA/external/phpids/0.6/lib/IDS/tmp/phpids\_log.txt

chmod 777 /home/wwwroot/default/DVWA/config

1. BIG-IP ASM策略配置
2. 首先通过 Security=>Event Logs=>Logging Profiles=>Create 创建ASM所需的Logging profile，如图1，图2所示。其中Server Addresses是BDE所在的IP和相应对接的端口。随后BDE中FLUENTD相应配置内容需要与Protocol、Server Addresses 、CSV delimiter和Storage Format的设定相匹配。

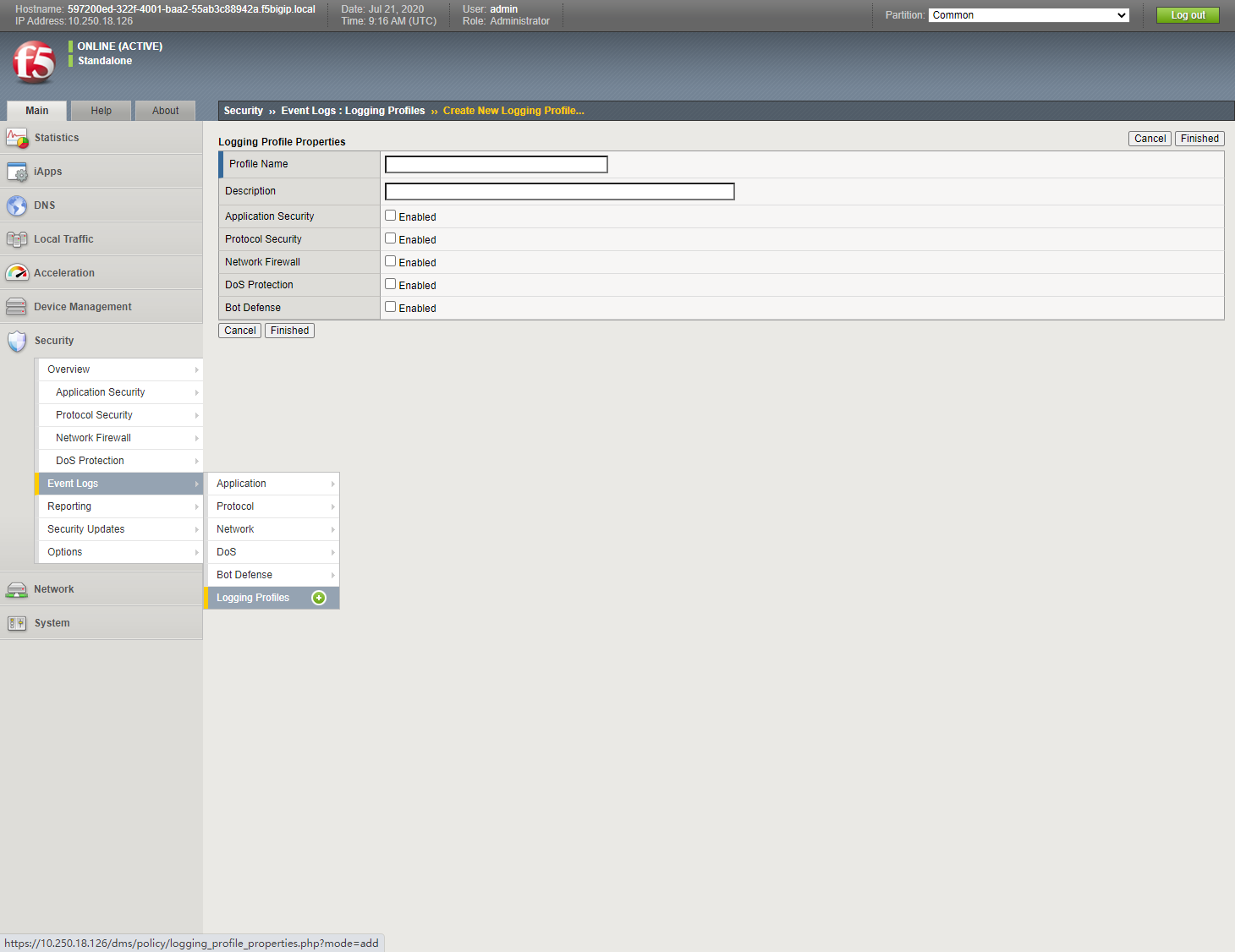


图1 创建ASM的Logging Profile

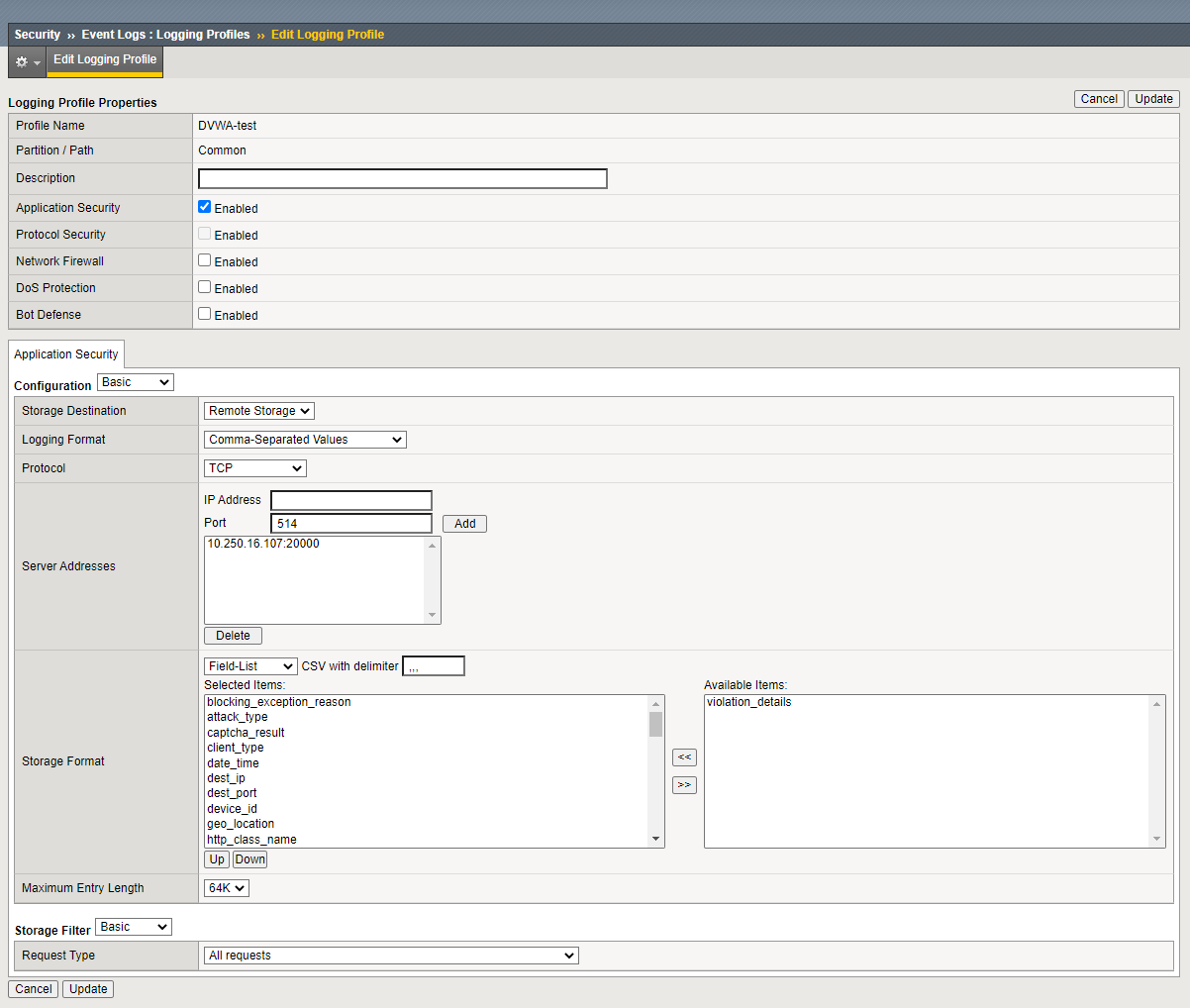


图2 配置ASM的Logging Profile

1. 通过Application Security=>Security Policies=>Create创建ASM策略。

首先选择Advanced模式；Policy Type选择Advanced；在VS的配置中，Logging Profile配置为刚刚在Event Logs中配置的规则，Pool Member配置为DVWA漏洞网站或者其他后台Web服务；Enforcement Mode为 Blocking；Signature Staging为Disabled。

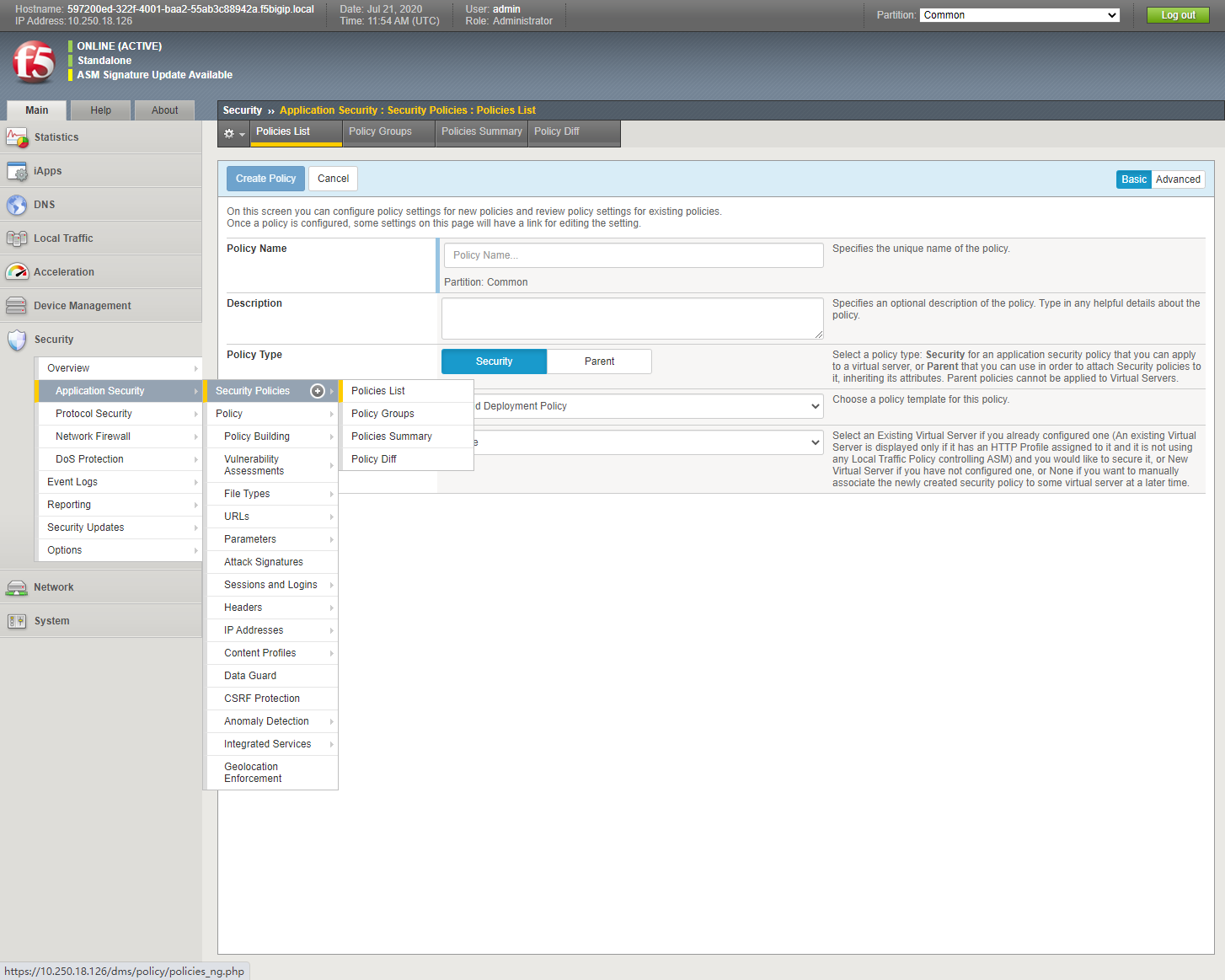


图3 创建ASM策略

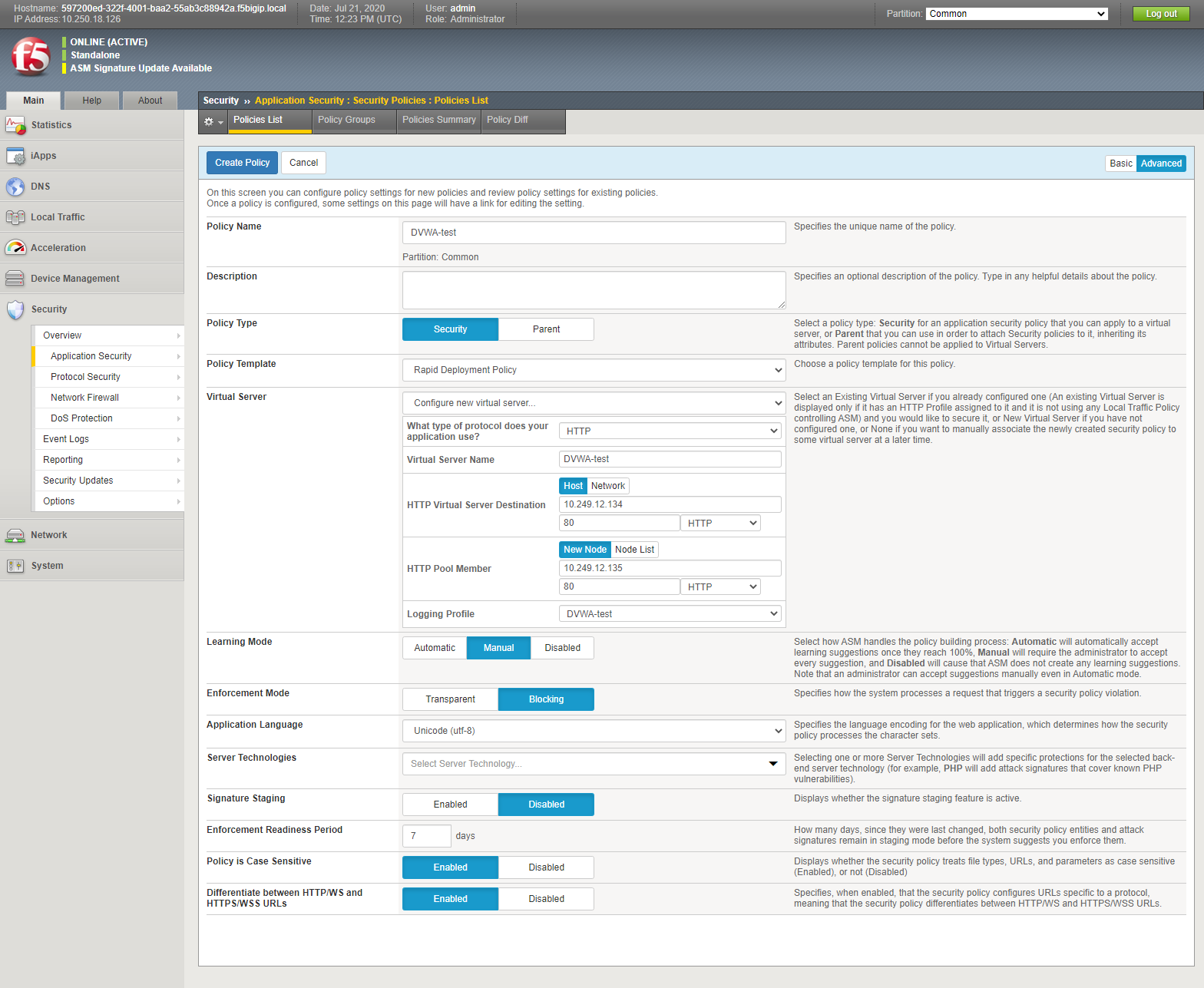


图4配置ASM策略（图中IP非真实IP）

1. BDE Fluentd相应配置

Fluentd相关配置如图5，首先协议类型、端口号要和BIG-IP ASM中的配置相匹配；然后Parse Type选为CSV，delimiter也和Logging Profile中配置保持一致（之所以这里使用“，，，”，是因为更容易对CSV字符串进行分割，以免处理异常）；Keys要和Logging Profile中Storage format的字段以及字段顺序保持一致。（第一个字段因为BIG-IP吐出的日志不是标准CSV格式会导致该字段数据可读性很差，所以第一个字段一般设为一个不常用字段）。

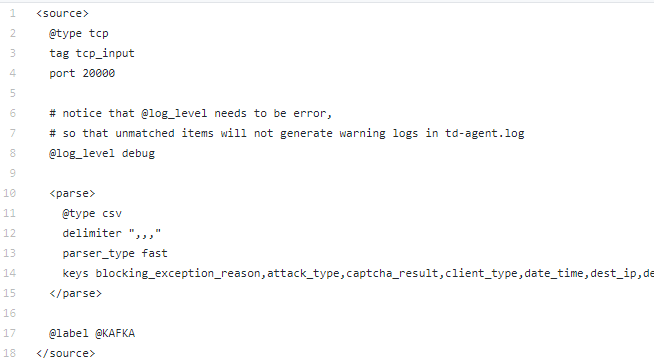


图5 Fluentd 对接ASM相应配置