我找到了旧版的用户手册，是v4，上面写的很清楚ossec和ossim怎么通信的，你手里的是v10或者更高版本吧，应该写的更详细点。

ossec分为client和server，client我们装在了宿主机上，server集成在ossim上，所以接下来可能会直接说ossim即指代ossec server端。同理snort也是有client和server， snort的client在宿主机上，server集成在ossim上。

1. 首先装ossec的时候就填写了ossim的ip，然后在ossim使用ossec\_agent 添加了ossim要监听的ossec宿主机。这个时候ossim和ossec就已经建立了联系。ossim默认开放1514端口会自动监听发送到该端口的数据即宿主机发送过来的各种日志（请搜索了解syslog转发日志）。

A screenshot of a cell phone

Description automatically generated

1. 在宿主机修改ossec配置文件，告诉ossec要发送宿主机哪些文件ossim，这个发送的内容是文件每次有更新都会发送，具体应该是文件指针变化。要发送的文件在/var/ossec/etc/ossec.conf中添加localfile，这个文件里面你还能看到很多ossec默认要发送给ossim的文件。

A screenshot of a cell phone

Description automatically generated

1. 在ossim开启日志接受功能，表示接受ossec客户端发送过来的文件。

A screenshot of a cell phone

Description automatically generated

1. 这个时候，所有的文件更新的内容都会以数据流的方式发送给ossim，在ossim那边它如果没有**相应规则**去解析它收到的数据，它就不知道这些数据到底有什么意义，会全部存放在/var/ossec/logs/archives/archives.log 目录下。
2. 如果有规则可以解析ossim收到的数据。观察到ossim的/var/ossec/logs/archives/arvhives.log里的内容：

A screenshot of a cell phone

Description automatically generated

可以看到，所有发送到ossim的数据，首先都会自动分析是什么时间从哪台宿主机发送过来的，格式：

日志接受时间+日志发送宿主机名称+日志发送宿主机ip+具体数据内容

Dec 14 08:23:04 volidsServerd: 10.10.26.185 7-ubuntu10044 warning {hidden modules? 0xffffffffa004ca20 rootkit}  
日期 时间 应用 检测虚拟机ip 检测虚拟机名称 日志等级 具体数据内容

在项目中，我们根据ossim解析日志的步骤自定义了volids.log里的日志结构即具体数据内容（这个volids.log里面日志为什么要这么定义，需要参考ossim规则是如何解析的，这部分一两句话说不清楚）：

Dec 14 08:23:04 volidsServerd: 10.10.26.185 7-ubuntu10044 warning {hidden modules? 0xffffffffa004ca20 rootkit}  
日期 时间 应用 检测虚拟机ip 检测虚拟机名称 日志等级 具体数据内容

* 1. 到这一步之后，就是添加规则来解析volids.log的具体数据内容。这个时候就用到了解码器decoder和具体规则。解码器decoder是解析特定的应用（在这里我们定义了volidsServerd），所有的decoder在 /var/ossec/alienvault/decoders 目录下。规则在/var/ossec/alienvault/rules 目录下，这里直接修改了local\_rules.xml 文件。