iMC通用syslog升级为告警的配置

PLAT 何颖 2013-04-23 发表

iMC通用syslog升级为告警的配置

一、 组网需求：

如何在大量的Syslog中提取关键信息是管理员面对的最大困难。Syslog管理系统预定义了大量规则，凡是符合这些规则的Syslog都将发送给iMC告警模块，经过告警模块过滤筛选的Syslog将升级为告警。告警可以帮助管理员定位并及时发现网络问题，快速定位到问题根源。用户对大量网络设备进行管理，在iMC中使用Syslog组件的相关功能的场景下推荐使用该功能。

无特殊组网需求。

二、 组网图：

无

三、 配置步骤：

用户可以针对Syslog特征，定制生成的告警。通过明显的告警特征，诊断故障根因，并通过查看相应Syslog报文的信息，可迅速定位故障的原因，大大缩短了用户故障处理的响应时间，从而提高用户的工作效率。可以通过增加含有Syslog报文特征的解析模板，然后增加升级为告警的规则，用户关心的Syslog在满足一定的条件后将会生成告警。具体配置步骤如下：

1. 首先进入解析模板库，在解析模板库中系统预订了一些关于安全类Syslog的解析模板，如：解析模板IP address collision，模板内容为“IP address $(Duplicate IP) collision detected, sourced by $(srcMAC) on $(Source IfDesc) of $(Source VLAN) and $(Peer MAC) on $(IfDesc) of $(VLAN)”。另外用户可以单击【增加】按钮，增加自己需要的解析模板。

图1 解析模板库界面

2. 单击【增加】按钮进入增加解析模板的页面，如图2所示，参考界面的提示信息增加解析模板。模板中支持输入参数，形式为$(参数名称)。这些参数将作为告警参数在告警中体现，便于用户定位故障原因。

图2 增加解析模板库

3. 点击左导航的【升级告警规则】，进入规则列表，如图3所示，系统预定义了一些过滤规则。如：规则Duplicate address 1，定义了重复间隔为300秒、重复次数为50、生成告警的级别为重要、解析模板为 Duplicate address $(Duplicate IP) on $(So

urce VLAN), sourced by $(srcMAC)。当收到的Syslog满足上述条件后，将会生成Syslog类的告警。另外用户可以单击【增加】按钮，增加自己需要的升级规则。

图3 升级告警规则页面

4. 单击【增加】按钮，进入增加规则页面。

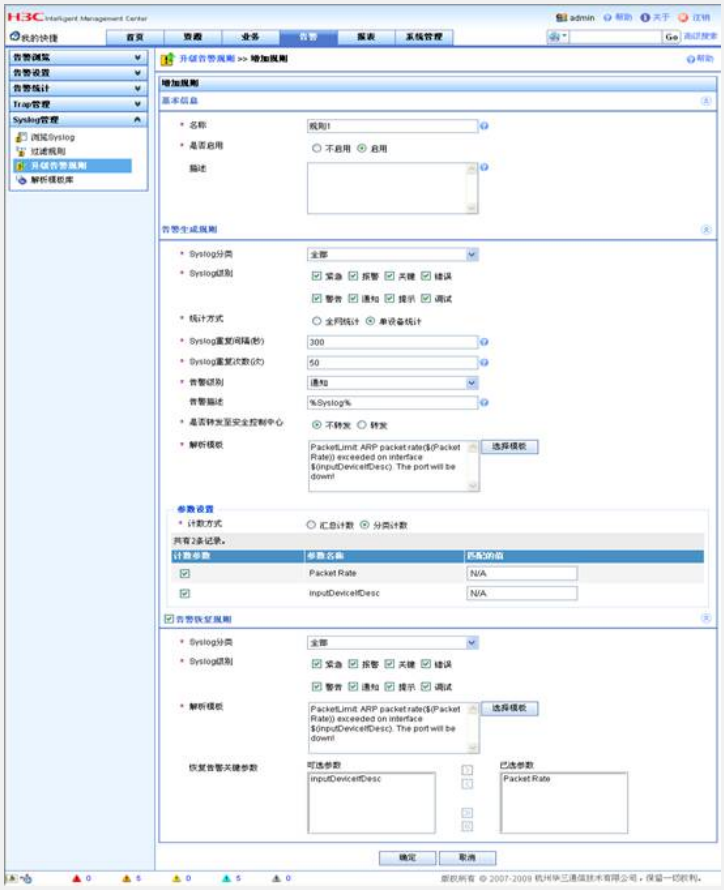

图4 增加规则界面

输入升级告警规则的相应信息，比如重复间隔、重复次数、解析模板等。增加规则成功后，iMC将按照规则描述，对生成的Syslog进行筛选、统计，将符合规则的Syslog生成相应的告警。

下面具体说明一下规则的工作机制：

1. iMC根据前面步骤中配置的规则筛选出符合规则的Syslog。符合规则的Syslog必须同时满足以下条件：

l Syslog必须属于规则中配置的Syslog分类。

l Syslog必须属于规则中配置的Syslog级别。

l Syslog必须包含规则中配置的解析模板的内容。

2. 判断Syslog是否包含解析模板的内容比较复杂，详细说明如下：

l 无论计数方式为汇总计数或分类计数，只要计数参数的匹配值设置为N/A，则对Syslog中具体的参数值没有要求。例如，解析模板为“PacketLimit: ARP packet rate($(Packet Rate)) exceeded on interface $(inputDeviceIfDesc). The port will be down!”其中包含了参数($(Packet Rate))，如果此参数的匹配值设置为N/A，则无论Syslog中Packet Rate的值是多少，都认为Syslog包含解析模板的内容。

l 无论计数方式为汇总计数或分类计数，只要计数参数的匹配值设置为某个具体的值，则Syslog中必须包含计数参数的值。例如，解析模板为“PacketLimit: ARP packet rate($(Packet Rate)) exceeded on interface $(inputDeviceIfDesc). The port will be down!”其中包含了参数($(Packet Rate))，如果此参数的匹配值设置为10，则Syslog中的Packet Rate的值为10，才判定Syslog包含解析模板的内容。

3. iMC对前面步骤中筛选出的符合规则的Syslog进行计数。如果统计方式选择全网统计，则整个网络中符合规则的Syslog统一计数；如果统计方式选择单设备统计，则每台设备产生的符合规则的Syslog分别计数。具体计数规则如下：

l 计数方式选择汇总计数，计数参数的匹配值设置为N/A，则对所有符合规则的Syslog进行合并计数。例如，Syslog 1计数参数为A、Syslog 2计数参数为B、Syslog 3计数参数为A，则Syslog计数为3。

l 计数方式选择汇总计数，计数参数的匹配值设置为具体的值，则对所有符合规则的Syslog进行合并计数。例如，计数参数匹配值设置为A，Syslog 1计数参数为A、Syslog 2计数参数为B、Syslog 3计数参数为A，则Syslog计数为2，Syslog 2因为计数参数不匹配被判定为不符合规则。

l 计数方式选择分类计数，计数参数的匹配值设置为N/A，则对计数参数不同的Syslog进行分别计数。例如，Syslog 1计数参数为A、Syslog 2计数参数为B、Syslog 3计数参数为A，则匹配参数A的Syslog计数为2，匹配参数B的Syslog计数为1。

l 计数方式选择分类计数，计数参数的匹配值设置为具体的值，则对符合规则的Syslog进行计数。例如，计数参数匹配值设置为A，Syslog 1计数参数为A、Syslog 2计数参数为B、Syslog 3计数参数为A，则Syslog计数为2，Syslog 2因为计数参数不匹配被判定为不符合规则。

当同一个计数在任意的“Syslog重复间隔”时间段内达到“Syslog重复次数”时，iMC产生告警。例如，Syslog重复间隔设置为60秒，Syslog重复次数设置为5次，则在任意连续的一分钟内，同一个Syslog计数达到5次，则iMC会产生告警。

如果在升级告警规则中配置了转发至安全控制中心，生成的告警将转发至安全控制中心，进行联动处理。

如果规则中配置了告警恢复，那么在收到符合该告警恢复条件的Syslog，会立即产生对应的恢复告警。为了使产生的恢复告警能够准确的恢复该规则先前产生的告警，建议指定恢复告警关键参数，该参数将作为产生的恢复告警的定位参数。定位参数是用来确定恢复告警和被恢复告警的存在恢复关系的字段。

四、 配置关键点：

无