#### syslog格式说明

Syslog的消息长度不超过1024字节。消息正文需要按照以下格式进行定义，其中字段之间用|+|隔开,如有字段为空系统将使用缺省值进行赋值。

具体格式如下：

事件集成系统名称|+|业务系统名称|+|管理机构|+|所属机构|+|节点IP|+|节点名称|+|事件名称|+|实例ID|+|实例值|+|组件类型|+|组件|+|组件子类|+|事件级别|+|事件描述|+|发生时间

（格式中颜色的含义: 蓝色：必填；黑色：选填。其中节点IP和节点名称至少需要其中一个，另外一个可为空，为空时填写字符NA，例如“...+|NA|+...”。格式中的内容不得包含“|”和“+”两种符号）

各字段的含义如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段名 | 描述 | 统一监控平台中ObjectSserver字段 |
| 1 | 事件集成系统名称 | 用于区分是报警的来源的应用系统，如：CEB-ECIF | Agent  ITSM，唯一 |
| 2 | 业务系统名称 | 用于区分报警所属于的业务系统，如：CEB-ECIF | N\_AppCode  业务系统名称，待定 |
| 3 | 管理机构 | 管理机构ID，若系统的管理机构为总行，填1001，若为分行，填分行机构号 | N\_MgtOrgId  总行，唯一  分行呆讨论 |
| 4 | 所属机构 | 所属机构ID，若系统的所属机构为总行，填1001，若为分行，填分行机构号。 | N\_OrgId  总行，唯一  分行呆讨论 |
| 5 | 节点IP | 节点IP，节点IP与节点名称必须填写一个 | NodeAlias \*  中间服务写死 |
| 6 | 节点名称 | 节点主机名，节点IP与节点名称必须填写一个 | N\_NodeName  不填 |
| 7 | 事件名称 | 标示具体报警策略分类，如具体脚本名 | N\_EventId \*  可恢复：xxx |
| 8 | 实例ID | 报警涉及的具体对象，如进程名、日志名、服务名、端口号、链路名、交易名、队列名等 | N\_InstanceId \*  应用id-应用名称  5、7、8组合成唯一标示，如果一致  {alert\_cluster-alert\_project-application} |
|  |  |  |  |
| 9 | 实例值 | 报警涉及的具体对象的状态，比如error/ok, 日志关键字等 | N\_InstanceValue  Error/ok ，90% |
| 10 | 组件类型 | 报警具体大类，比如APP、NETWORK、DB、OS、SECURITY、STORAGE、HARDWARE | N\_ComponentTypeId  App  写死 APP |
| 11 | 组件 | 报警应用名称，如ECIF、LINUX、ORACLE | N\_ComponentId  容器云 写死 CPAAS |
| 12 | 组件子类 | 报警细类，必须大写，对于ECIF报警，子类包含  进程(Process)：PROCESS  端口(Port)：PORT  服务(Service)：SERVICE  对于LINUX如CPU、Memory等  对于Oracle如表空间等 | N\_SubComponentId  报指标名。。。  {alert\_indicator} |
| 13 | 事件级别 | 1级（故障）电话并会建事件单  2级（报警）电话沟通  3级（预警）短信通知/app  4级（提示）提醒  100级（信息） | N\_CustomerSeverity  恢复100； |
| 14 | 事件描述 | 报警事件的具体描述信息，可以是中文 | N\_SummaryCN  中文描述 |
| 15 | 发生时间 | 报警发生时间，建议使用utf时间（到1970-1-1的秒数） | FirstOccurence |

***注：表格中红色字体为告警事件的主键组合字段***

举例如下：

发送syslog命令

logger -t 2OMNIBUS -p local7.debug "CEB-ECIF|+|CEB-ECIF|+|1001|+|1001|+|NA|+|$APPX|+|app\_core\_check.sh|+|core|+|coredump|+|APP|+|ECIF|+|PROCESS|+|2|+| APPX-CORE error -/home/ecisrv/bin/core |+|$TIMESTAMP"

输出结果

06 15 14:33:46 10.1.41.6 **2OMNIBUS:** CEB-ECIF|+|CEB-ECIF|+|1001|+|1001|+|NA|+|sd13pp1|+|app\_core\_check.sh|+|core|+|coredump|+|APP|+|ECIF|+|PROCESS|+|3|+|APPX-CORE error -/home/ecisrv/bin/core|+|1339751273

Logger发送方式中需增加-t参数来标识事件的来源。程序开发时也应增加事件来源标识，如上面例子中的2OMNIUBS标识了ECIF集成平台发送的事件，该标识与后面拼接的事件内容用空格做区分。另外如需发送中文，建议使用UTF8编码格式。