Syslog格式扩展规范

|  |  |  |  |
| --- | --- | --- | --- |
| 修订版本记录 | | | |
| 文档版权 | 北京天地和兴科技有限公司 | | |
| 发布日期 | 版本 | 修订内容说明 | 修订人 |
| 2017/3/7 | V1.0 | 创建扩展格式 | 梁杰 |
|  |  |  |  |

## 一、前言

Syslog标准格式包含三部分：PRI,HEADER,MSG，MSG部分包括TAG和CONTENT两个字段，我们的扩展格式添加到MSG字段的CONTENT部分后面，以“｜”与CONTENT 字段分隔。

## 二、标准格式与扩展

现在程序中包含四类日志：进程白名单预警日志、移动存储访问预警日志、用户操作日志、windows系统日志。

2.1日志分类和版本定义：

|  |  |  |
| --- | --- | --- |
| 日志分类 | 字段标示符 | 版本号 |
| 进程白名单预警日志 | S | 1 |
| 移动存储访问预警日志 | U | 1 |
| 用户操作日志 | O | 1 |
| windows系统日志 | W | 1 |

2.2 日志类型

我们获取了windows的系统、安全、应用程序、Setup等日志，用整数代表windows日志的类型进行传输，有效减少数据包量。

|  |  |  |
| --- | --- | --- |
| Windows系统日志类型 | 数据类型 | 对应的值 |
| 成功 | 16进制整数 | 0x00 |
| 错误 | 16进制整数 | 0x01 |
| 警告 | 16进制整数 | 0x02 |
| 信息 | 16进制整数 | 0x04 |
| 审核成功 | 16进制整数 | 0x08 |
| 审核失败 | 16进制整数 | 0x10 |

2.3 Syslog标准与扩展格式如下所示：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 字段顺序 | 字段说明 | 进程白名单预警日志 | 移动存储访问预警日志 | 用户操作日志 | windows系统日志 | 备注 |
| 1 | Syslog标准格式的PRI字段 | 具体格式及内容见4.1描述 | 具体格式及内容见4.1描述 | 具体格式及内容见4.1描述 | 具体格式及内容见4.1描述 | Syslog的标准格式，以尖括号分隔 |
| 2 | Syslog标准格式的HEADER字段的时间部分 | 包含年月日时分秒 | 包含年月日时分秒 | 包含年月日时分秒 | 包含年月日时分秒 | 这个字段以空格符分隔，第一段是月份的英语简写，第二段是日，第三段是时、分、秒，如果在时分秒后面有CST字段，则下一字段是年份，否则时分秒后为计算机名或IP |
| 3 | Syslog标准格式的HEADER字段的计算机名或IP部分 | 计算机名 | 计算机名 | 计算机名 | 计算机名 |  |
| 4 | Syslog标准格式的MSG字段的进程名部分 | 引起预警的进程名 | 移动存储的盘符或路径 | 执行操作的用户名 | Windows日志的类型名（系统日志、安全日志、应用日志、安装日志） | 进程名以冒号（：）结束 |
| 5 | Syslog标准格式的MSG字段的描述内容部分 | 预警产生的描述信息 | 预警产生的描述信息 | 操作的相应说明 | 日志的描述信息 | 这个字段后面为扩展内容，以竖杠（“｜”）分隔 |
| 6 | 日志类型标志 | S | U | O | W | 用字母表示日志的类型，节省传输带宽 |
| 7 | 扩展协议的版本 | 1 | 1 | 1 | 1 | 用于协议以后的再扩展 |
| 8 | 扩展内容1 | 进程文件所属的公司名 | -- | -- | 日志类型见2.2节表 | 与前后字段以竖杠（“｜”）分隔 |
| 9 | 扩展内容2 | 进程文件的版本号 | -- | -- | 事件ID号 | 与前后字段以竖杠（“｜”）分隔 |
| 10 | 扩展内容3 | 进程文件的大小 | -- | -- | 事件来源 | 与前后字段以竖杠（“｜”）分隔 |
| 11 | 扩展内容4 | 进程文件的全路径 | -- | -- | 用户名 | 与前后字段以竖杠（“｜”）分隔 |

注： -- 代表没有此项

## 三、格式示例

3.1 进程白名单预警日志的格式，

<30>Mar 7 12:33:20 CST 2017 win2008x64 notepad.exe: 非白名单程序预警运行|S|1|Microsoft Corporation|6.3.9600.17930|216KB|C:\Windows\System32

3.2移动存储访问预警日志的格式

<4>Mar 7 11:03:21 CST 2017 win2008x64 E: 非白名单U盘禁用|U|1

3.3用户操作日志

<13>Mar 7 15:11:05 CST 2017 win2008x64 Admin: 执行白名单程序入库|O|1

3.4 windows系统日志

<28>Mar 7 17:02:20 CST 2017 win2008x64 System: Inter(R) Ethernet Connection I218-V|W|1|4|32|e1dexpress|N/A

## Syslog标准格式概述

4.1 PRI字段由两部分构成，这个数字包含了程序模块（Facility）、严重性（Severity），这个数字是由Facility乘以8然后加上Severity得来，即是高5位代表Facility，低3位代表Severity，Facility定义如下：

Numerical             Facility  
         Code  
  
          0             kernel messages  
          1             user-level messages  
          2             mail system  
          3             system daemons  
          4             security/authorization messages (note 1)  
          5             messages generated internally by syslogd  
          6             line printer subsystem  
          7             network news subsystem  
          8             UUCP subsystem  
          9             clock daemon (note 2)  
         10             security/authorization messages (note 1)  
         11             FTP daemon  
         12             NTP subsystem  
         13             log audit (note 1)  
         14             log alert (note 1)  
         15             clock daemon (note 2)  
         16             local use 0  (local0)  
         17             local use 1  (local1)  
         18             local use 2  (local2)  
         19             local use 3  (local3)  
         20             local use 4  (local4)  
         21             local use 5  (local5)  
         22             local use 6  (local6)

根据我们日志的来源（来自用户或内核模式）转换相应的值。

Sevirity的定义如下：

Numerical         Severity  
        Code  
  
        0       Emergency: system is unusable  
          1       Alert: action must be taken immediately  
        2       Critical: critical conditions  
          3       Error: error conditions  
          4       Warning: warning conditions  
          5       Notice: normal but significant condition  
        6       Informational: informational messages  
          7 Debug: debug-level messages

PRI的格式是数字加上尖括号，如下所示：

<30>

4.2 HEADER部分

HEADER部分包括时间与主机名，时间是由月、日、时、分、秒组成（由于标准的格式中没有年份，所以首先确定服务端能否解析年字符串，才能确定是否能添加年份），HEADER的格式如下所示：

Aug 24 05:34:00 CST 1987 mymachine

* 1. MSG部分

MSG部分包括TAG和CONTENT，TAG包含的是进程名和进程ID信息，可以没有进程ID，CONTENT包含这条日志的说明信息，MSG格式如下所示：

Auditd.exe: The audit daemon is exiting