

问题描述

CAS syslog服务器接收信息分类

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.10.1	10.10.10.1	Syslog	242	KERN.ERR: 2022-06-24 16:23:09 3
2	4.707376	10.10.10.1	10.10.10.1	Syslog	242	KERN.ALERT: 2022-06-24 16:23:14
3	4.709466	10.10.10.1	10.10.10.1	Syslog	275	KERN.ALERT: 2022-06-24 16:23:14
4	4.863137	10.10.10.1	10.10.10.1	Syslog	242	KERN.ERR: 2022-06-24 16:23:14 3
5	4.898219	10.10.10.1	10.10.10.1	Syslog	253	KERN.ALERT: 2022-06-24 16:23:14
6	5.027403	10.10.10.1	10.10.10.1	Syslog	242	KERN.ERR: 2022-06-24 16:23:14 3
7	5.042091	10.10.10.1	10.10.10.1	Syslog	242	KERN.ERR: 2022-06-24 16:23:14 3
8	5.189845	10.10.10.1	10.10.10.1	Syslog	242	KERN.ERR: 2022-06-24 16:23:14 3
9	7.947020	10.10.10.1	10.10.10.1	Syslog	274	KERN.ERR: 2022-06-24 16:23:17 3
...	10.079988	10.10.10.1	10.10.10.1	Syslog	243	KERN.ALERT: 2022-06-24 16:23:19 1
...	21.765897	10.10.10.1	10.10.10.1	Syslog	253	KERN.ERR: 2022-06-24 16:23:31 3
...	28.770423	10.10.10.1	10.10.10.1	Syslog	185	KERN.INFO: 2022-06-24 16:23:38 6
...	29.545012	10.10.10.1	10.10.10.1	Syslog	274	KERN.ALERT: 2022-06-24 16:23:39 1
...	33.428037	10.10.10.1	10.10.10.1	Syslog	242	KERN.ALERT: 2022-06-24 16:23:43 1
...	33.534988	10.10.10.1	10.10.10.1	Syslog	242	KERN.ALERT: 2022-06-24 16:23:43 1
...	33.552742	10.10.10.1	10.10.10.1	Syslog	242	KERN.ALERT: 2022-06-24 16:23:43 1
...	33.663095	10.10.10.1	10.10.10.1	Syslog	242	KERN.ALERT: 2022-06-24 16:23:43 1
...	33.683527	10.10.10.1	10.10.10.1	Syslog	242	KERN.ALERT: 2022-06-24 16:23:43 1

#### 解决方法

- 1、KERN.INFO: 对应操作日志
- 2、KERN.WARNING: 对应次要告警
- 3、KERN.ALERT: 对应重要告警
- 4、KERN.EMERG: 对应紧急告警

