LabrisAdministrativeRecorder Column Mappings

Jul 22 20:38:14 2010 sshd[8243]: Accepted password for natek from 192.168.20.6 port 51352 ssh2

ID	
EVENT_ID	
RECORD_NUMBER	
EVENTYPE	
EVENTCATEGORY	**Accepted password**
DATE_TIME	**Jul 22 20:38:14 2010**
DESCRIPTION	**ssh2**
SOURCENAME	
COMPUTERNAME	
USERSID	
LOG_NAME	
CUSTOMSTR1	**natek(user)**
CUSTOMSTR2	
CUSTOMSTR3	**192.168.20.6 (source)**
CUSTOMSTR4	**Labrisin IP**
CUSTOMSTR5	
CUSTOMSTR6	
CUSTOMSTR7	
CUSTOMSTR8	
CUSTOMSTR9	
CUSTOMSTR10	
CUSTOMINT1	**51352 (port)**
CUSTOMINT2	**8243 (unique)**
CUSTOMINT3	
CUSTOMINT4	
CUSTOMINT5	
CUSTOMINT6	
CUSTOMINT7	
CUSTOMINT8	
CUSTOMINT9	
CUSTOMINT10	
SIGN	
SIGN_TIME	
SEVERITY	
TAXONOMY	

Labrisin IP'sini bulmamız gerek. Loga düşmüyo. Gelen makşnenin ıpsi alınacak. ----> customstr4

administrative kayıt eder dolduğu zaman dosyanın sonuna .1 gibi sıralı bir şekilde sayı koyup administrative dosyasını temizler.

nezih.unal@natek.com.tr