İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc329872435)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc329872436)

[ÖRNEK PARSING 4](#_Toc329872437)

[TEMEL PARSING YAPISI 6](#_Toc329872438)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
| 25.06.2013 | Version 1.0 |  | Ali BOZDAĞ |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | Juniper SRX 220 |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | JuniperSyslogSRX220V\_1\_0\_0Recorder.dll |
| İstek yapan Adı Soyadı | Ali BOZDAĞ |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 25.06.2013 |
| İstek yapılan kurum adı | Ankara Kalkınma Ajansı |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | Syslog |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları |  |

# ÖRNEK PARSING -1

|  |  |
| --- | --- |
| 192.168.2.1:50661 : local7.warning Jun 25 14:21:45 AnkKalk utmd[1186]: WEBFILTER\_URL\_BLOCKED: WebFilter: ACTION="URL Blocked" 192.168.1.176(49549)->92.45.106.141(80) CATEGORY="Advertisements" REASON="by predefined category" PROFILE="junos-wf-cpa-default" URL=adsp.haberturk.com OBJ=/advertpro/servlet/file?id=5097  192.168.2.1:63963 : local7.info Jun 25 14:30:51 AnkKalk utmd[1186]: WEBFILTER\_URL\_PERMITTED: WebFilter: ACTION="URL Permitted" 192.168.1.176(50003)->141.101.112.14(80) CATEGORY="N/A" REASON="by other category" PROFILE="junos-wf-cpa-default" URL=www.yabancidiziizle.net OBJ=/reklam/300x250-4.php  192.168.2.1:63963 : local7.warning Jun 25 14:30:55 AnkKalk utmd[1186]: WEBFILTER\_URL\_PERMITTED: WebFilter: ACTION="URL Permitted" 192.168.4.8(43438)->173.194.70.113(443) CATEGORY="Search\_Engines" REASON="by predefined category" PROFILE="restricted\_category" URL=173.194.70.113 OBJ=/ | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | Jun 25 14:21:45 |
| SOURCENAME |  |
| EVENTCATEGORY | warning |
| EVENTTYPE | WEBFILTER\_URL\_BLOCKED |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | AnkKalk |
| CUSTOMSTR1 | URL Blocked |
| CUSTOMSTR2 | Advertisements |
| CUSTOMSTR3 | 192.168.1.176 |
| CUSTOMSTR4 | 92.45.106.141 |
| CUSTOMSTR5 | by predefined category |
| CUSTOMSTR6 | adsp.haberturk.com |
| CUSTOMSTR7 | /advertpro/servlet/file?id=5097 |
| CUSTOMSTR8 | junos-wf-cpa-default |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | 49549 |
| CUSTOMINT4 | 80 |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

# TEMEL PARSING -1

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 |  |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

# ÖRNEK PARSING -2

|  |  |
| --- | --- |
| 192.168.2.1:64248 : local7.info Jun 25 14:51:02 AnkKalk RT\_FLOW: RT\_FLOW\_SESSION\_CLOSE: session closed TCP FIN: 192.168.1.140/62694->199.59.150.39/443 junos-https 212.175.34.170/15273->199.59.150.39/443 rule1 None 6 AccessToInternet ClientSide ADSL 42683 12(3005) 13(1161) 34 UNKNOWN UNKNOWN N/A(N/A) ge-0/0/6.0  192.168.2.1:64248 : local7.info Jun 25 14:51:02 AnkKalk RT\_FLOW: RT\_FLOW\_SESSION\_CLOSE: session closed TCP FIN: 192.168.1.122/49669->23.62.53.43/80 junos-http 212.175.34.170/10228->23.62.53.43/80 rule1 None 6 AccessToInternet ClientSide ADSL 87321 9(2717) 11(9978) 55 UNKNOWN UNKNOWN N/A(N/A) ge-0/0/6.0  192.168.2.1:64248 : local7.info Jun 25 14:58:27 AnkKalk RT\_FLOW: RT\_FLOW\_SESSION\_CREATE: session created 192.168.4.6/50057->195.175.69.89/80 junos-http 212.175.34.170/25727->195.175.69.89/80 rulewireless None 6 WirelessAccess LokalWireless ADSL 42359 N/A(N/A) ge-0/0/7.2 | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | Jun 25 14:51:02 |
| SOURCENAME |  |
| EVENTCATEGORY | İnfo 2 |
| EVENTTYPE | RT\_FLOW 7 |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | AnkKalk 6 |
| CUSTOMSTR1 | session closed |
| CUSTOMSTR2 | junos-https 14 |
| CUSTOMSTR3 | 192.168.1.140 |
| CUSTOMSTR4 | 199.59.150.39 |
| CUSTOMSTR5 | 212.175.34.170 |
| CUSTOMSTR6 | 199.59.150.39 |
| CUSTOMSTR7 | rule1 |
| CUSTOMSTR8 | ge-0/0/6.0 |
| CUSTOMSTR9 | AccessToInternet ClientSide ADSL |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | 62694 |
| CUSTOMINT4 | 443 |
| CUSTOMINT5 | 15273 |
| CUSTOMINT6 | 443 |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

# TEMEL PARSING -2

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 |  |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |