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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | F5 |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | F5SyslogV\_1\_0\_0Recorder.dll |
| İstek yapan Adı Soyadı | Nezih Ünal |
| Geliştirici Adı Soyadı |  |
| İstek tarihi |  |
| İstek yapılan kurum adı | Emniyet Genel Müdürlüğü |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi |  |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları |  |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| **s\_ip=78.189.233.157:s\_port=8016:d\_ip=192.168.125.10:d\_port=80:host=www.elazig.pol.tr:url=/SiteAssets/Iller/Images/AnaMenuSolLine.png: method=GET: time=2013/05/06\*16:48:58** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **2013/05/06\*16:48:58** |
| SOURCENAME | **www.elazig.pol.tr** |
| EVENTCATEGORY |  |
| EVENTTYPE | **GET** |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **78.189.233.157** |
| CUSTOMSTR4 | **192.168.125.10** |
| CUSTOMSTR5 | **/SiteAssets/Iller/Images/AnaMenuSolLine.png --- 900 kontrolü aşan str6 ya** |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | **8016** |
| CUSTOMINT4 | **80** |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full log – 4000 kontrolü yapılacak artan kısım str10 a basılacak |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME | DATE\_TIME |
| SOURCENAME | Site hostname |
| EVENTCATEGORY |  |
| EVENTTYPE | Method – get/post |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | Source ip |
| CUSTOMSTR4 | Local server ip |
| CUSTOMSTR5 | url - subpage |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | Source port |
| CUSTOMINT4 | Local server port |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full log |

F5 ürününde log konfigurasyonu olarak aşağıdaki tanım girilmiştir.

**when CLIENT\_ACCEPTED {**

**set hsl [HSL::open -proto UDP -pool pool\_syslog]**

**}**

**when HTTP\_REQUEST {**

**HSL::send $hsl "s\_ip=[IP::client\_addr];s\_port=[TCP::client\_port];d\_ip=[IP::local\_addr];d\_port=[TCP::local\_port];host=[HTTP::host];url=[HTTP::uri];method=[HTTP::method]; time=[clock format [clock seconds] -format %Y/%m/%d\*%H:%M:%S]"**

**}**

