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 |
|  |  |  |  |
| 08.01.2012 | V.1 | Beşiktaş Belediyesi için Squid loğlarının syslog ile alımının yapılması gerekmektedir. | Emrehan Mert |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | - |
| Ürün Adı | PFSENSE Proxy |
| Versiyonu | Current: 2.7.9 pkg v.4.3.1 Installed: 2.7.9\_4.1 |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | SquidSyslogV\_1\_0\_0Recorder |
| İstek yapan Adı Soyadı | Emrehan Mert |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 08.01.2012 |
| İstek yapılan kurum adı | Beşiktaş Belediyesi |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no | - |
| İlgili ham log yolu/dosya ismi | pfsense proxy\_yeni.txt |
| İlişkili form adı | - |
| Servis Yetkilisi Notları | - |
| Geliştirici Notları | - |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| **172.16.1.25:514 : local4.info Jan 7 13:53:09 squid[44380]: 1357559589.677 1117 172.16.10.115 TCP\_MISS/200 16071 GET http://www.google.com.tr/extern\_chrome/e1b299cac46c21f3.js - DIRECT/173.194.70.94 text/javascript** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | Jan 7 13:53:09 |
| SOURCENAME |  |
| EVENTCATEGORY | TCP\_MISS/200 |
| EVENTTYPE | GET |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | **http://www.google.com.tr/extern\_chrome/e1b299cac46c21f3.js** |
| CUSTOMSTR2 | **text/javascript** |
| CUSTOMSTR3 | **172.16.10.115** |
| CUSTOMSTR4 | **DIRECT/173.194.70.94** |
| CUSTOMSTR5 | **local4.info** |
| CUSTOMSTR6 | **1357559589.677** |
| CUSTOMSTR7 | **squid[44380]:** |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 | **172.16.1.25:514** |
| CUSTOMINT1 |  |
| CUSTOMINT2 | **1117** |
| CUSTOMINT3 | **16071** |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 172.16.1.25:514 : local4.info Jan 7 13:53:09 squid[44380]: 1357559589.677 1117 172.16.10.115 TCP\_MISS/200 16071 GET http://www.google.com.tr/extern\_chrome/e1b299cac46c21f3.js - DIRECT/173.194.70.94 text/javascript |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **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 |  |