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 |
| 19.04.2013 | Version 1.2 | JuniperSyslogV6\_0\_0Recorder.dll ile Alınan Juniper Firewall Loglarına DHCP Loglarının da Eklenmesi | Emre BAŞTUĞ |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | Juniper NS-5GT ve SSG Ürünleri |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | JuniperSyslogV6\_0\_1Recorder.dll |
| İstek yapan Adı Soyadı | Emre BAŞTUĞ |
| Geliştirici Adı Soyadı |  |
| İstek tarihi | 29.04.2013 |
| İstek yapılan kurum adı | Pendik Belediyesi |
| 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

|  |  |
| --- | --- |
| 2013-04-19 14:42:57 info IP address 192.168.56.104 is assigned to b8a386531dae. | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 2013-04-19 14:42:57 |
| SOURCENAME |  |
| EVENTCATEGORY | info |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 | assigned |
| CUSTOMSTR3 | 192.168.56.104 |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 | b8a386531dae |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 2013-04-19 14:42:57 info IP address 192.168.56.104 is assigned to b8a386531dae |

# TEMEL PARSING -1

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME | Tarih |
| SOURCENAME |  |
| EVENTCATEGORY | Firewall Log Seviyesi |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 | Ip assign bilgisi |
| CUSTOMSTR3 | Assing edilen IP adresi |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 | IP adresini alan client PC MAC bilgisi |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

# ÖRNEK PARSING -2

|  |  |
| --- | --- |
| 192.168.15.1:50872 : local0.info ssg20: NetScreen device\_id=0164122011000586 [Root]system-information-00527: IP address 192.168.15.84 is assigned to 9494261031e5. (2013-04-29 16:42:36) | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 2013-04-19 14:42:57 |
| SOURCENAME | 192.168.15.1:50872 |
| EVENTCATEGORY |  |
| EVENTTYPE | system-information-00527 |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | ssg20 |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 | assigned |
| CUSTOMSTR3 | 192.168.56.104 |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 | local0.info |
| CUSTOMSTR9 | 9494261031e5 |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 192.168.15.1:50872 : local0.info ssg20: NetScreen device\_id=0164122011000586 [Root]system-information-00527: IP address 192.168.15.84 is assigned to 9494261031e5. (2013-04-29 16:42:36) |

# TEMEL PARSING -2

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME | Tarih |
| SOURCENAME | Firewall IP Adresi |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | Firewall Modeli |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 | Ip assign bilgisi |
| CUSTOMSTR3 | Assing edilen IP adresi |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 | Vlan name |
| CUSTOMSTR9 | IP adresini alan client PC MAC bilgisi |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |