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 | Linux DNS |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi |  |
| İstek yapan Adı Soyadı | Nezih Ünal |
| Geliştirici Adı Soyadı |  |
| İstek tarihi |  |
| İstek yapılan kurum adı |  |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi |  |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları |  |

# TİP 1

# ÖRNEK PARSING

|  |  |
| --- | --- |
| **Dec 15 06:43:59 atadnsic named[17369]: DNS format error from 68.142.254.15#53 resolving login-global.lgg1.b.yahoo.com/AAAA for client 172.16.10.11#9859: invalid response** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Dec 15 06:43:59 – Yıl bilgisi olarak bulunulan yıl eklenebilir.** |
| SOURCENAME | **atadnsic** |
| EVENTCATEGORY | **DNS format error** |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | **login-global.lgg1.b.yahoo.com/AAAA** |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **172.16.10.11** |
| CUSTOMSTR4 | **68.142.254.15** |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | **9859** |
| CUSTOMINT4 | **53** |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | FULL LOG BASILACAK |

# TİP 2

# ÖRNEK PARSING

|  |  |
| --- | --- |
| **Dec 15 06:43:59 atadnsic named[17369]: error (FORMERR) resolving ‘login-global.lgg1.b.yahoo.com/AAAA/IN’: 68.180.130.15#53** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Dec 15 06:43:59 – Yıl bilgisi olarak bulunulan yıl eklenebilir.** |
| SOURCENAME | **atadnsic** |
| EVENTCATEGORY | **error** |
| EVENTTYPE | **FORMERR** |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | **‘login-global.lgg1.b.yahoo.com/AAAA/IN** |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 |  |
| CUSTOMSTR4 | **68.180.130.15** |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 | **53** |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full log basılacak |

# Tip 3

# ÖRNEK PARSING

|  |  |
| --- | --- |
| **Dec 15 06:49:40 atadnsic named[17369]: lame server resolving 'www.zorlasik.com' (in 'zorlasik.com'?): 72.20.15.129#53** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Dec 15 06:49:40 – yıl bilgisi olarak bulunulan yıl eklenebilir.** |
| SOURCENAME | **atadnsic** |
| EVENTCATEGORY | **lame server resolving** |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | **www.zorlasik.com** |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 |  |
| CUSTOMSTR4 | **72.20.15.129** |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 | **53** |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full log basılacak |

# Tip 4

# ÖRNEK PARSING

|  |  |
| --- | --- |
| **Dec 15 12:18:35 atadnsic named[17369]: success resolving 'dns3.repar.com/AAAA' (in 'repar.com'?) after disabling EDNS** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Dec 15 12:18:35 – yıl bilgisi olarak bulunulan yıl eklenebilir.** |
| SOURCENAME | **atadnsic** |
| EVENTCATEGORY | **success resolving** |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | **dns3.repar.com/AAAA** |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 |  |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full log basılacak |

# Tip 5

# Yukarıdaki formatlara uymayan bütün loglar için aşağıdaki parse yapısı kullanılmalı

# ÖRNEK PARSING

|  |  |
| --- | --- |
| **Dec 15 06:43:58 atadnsic rsyslogd: [origin software="rsyslogd" swVersion="5.8.6" x-pid="482" x-info="http://www.rsyslog.com"] rsyslogd was HUPed** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Dec 15 06:43:58 – yıl bilgisi olarak bulunulan yıl eklenebilir.** |
| SOURCENAME | **atadnsic** |
| 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 basılacak |

# 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 |  |