# RECORDER GELİŞTİRME İSTEK FORMU

|  |
| --- |
| Ürün Adı: Juniper SSL VN |
| Versiyonu: MAG 2600 |
| Log Toplama Tipi: Syslog |

# 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 |  |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| **172.34.1.6:514** : **local0.info** Juniper: 2002-04-04 02:04:02 - ive - [**92.45.222.100**] TOROSTRM\ozkan(**Users Realm**)[**Baan Role**] - **WebRequest completed**, GET to http://172.34.1.63:80//webui/servlet/login from 172.34.1.63 result=200 sent=33 received=1647 in 0 seconds | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME \* | 2002-04-04 02:04:02 |
| SOURCENAME | **local0.info** |
| EVENTCATEGORY | **System / Account / Login / WebRequest ( koşula bağlı biz yazacağız)** |
| EVENTTYPE \* | Information |
| USERSID \* | TOROSTRM\ozkan |
| LOGNAME | JuniperSSLVpnRecorder |
| COMPUTERNAME | **172.34.1.6:514** |
| CUSTOMSTR1 | **WebRequest completed** |
| CUSTOMSTR2 \* | **Users Realm** |
| CUSTOMSTR3 \* | **92.45.222.100** |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 \* | **Baan Role** |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | 172.34.1.63 |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | 200 |
| CUSTOMINT4 | 33 |
| CUSTOMINT5 | 1647 |
| CUSTOMINT6 | 0 |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 | GET |
| CUSTOMINT10 | http://172.34.1.63:80//webui/servlet/login |
| DESCRIPTION | Full log basılacak |

Ek Açıklamalar:

11 farklı veri var bunların her biri kendi içinde tekrarsız ve birinden ayrı bilgiler. Syslog mesajında aşağıda stingler var ise her biri ayrı ayrı değerlendirilecek. Yoksa Description gelen log basılacak.

1. Number of concurrent users logged in to the device
2. Number of JCP connections
3. Number of NCP connections
4. User Accounts modified
5. User Accounts modified
6. Login succeeded
7. Login failed
8. Login failed
9. Session timed out
10. WebRequest ok
11. WebRequest completed

**Devamı aşağıdaki gibidir.**

Standart olarak hepsinde ilk kısımlar benzer.

**172.34.1.6:514** : **local0.info** Juniper: 2002-04-04 02:04:02 - ive - [**92.45.222.100**] TOROSTRM\ozkan(**Users Realm**)[**Baan Role**]

**172.34.1.6:514 :** İlk iki nokta üst üste gelince kadar olan kısım her zaman COMPUTERNAME ’ye gidecek.

**local0.info** : Bu ifade genel olup her zaman SOURCENAME ‘e gidecek.

2002-04-04 02:04:02: Her zaman DATE\_TIME alanına gidecek.

**92.45.222.100** : ilk köşeli parantez içerisinde yer alır “[….]”. Her zaman CUSTOMSTR3 ‘e.

TOROSTRM\ozkan: ilk “**]**” karakteri sonrası ve ilk “**(**“ karakteri arasında yer alır. USERSID

**Users Realm** : ilk “()” parantez bloğunda yer alır. Her zaman CUSTOMSTR2 ‘e.

**Baan Role** : ikinci köşeli parantez içerisinde yer alır “[….]”. Her zaman CUSTOMSTR5 ‘e.

Mesajta “Number of concurrent users logged in to the device” varsa:

Kırmızı yazılı ifade **CUSTOMSTR1**’e, ifadenin akabindeki “:” den sonraki sayısal değer **CUSTOMINT1**’e ve **EVENTCATEGORY** kısmınıda “System” yazılacak.

Mesajta “Number of JCP connections” varsa:

Kırmızı yazılı ifade **CUSTOMSTR1**’e, ifadenin akabindeki “:” den sonraki sayısal değer **CUSTOMINT1**’e ve **EVENTCATEGORY** kısmınıda “System” yazılacak.

Mesajta “Number of NCP connections” varsa:

Kırmızı yazılı ifade **CUSTOMSTR1**’e, ifadenin akabindeki “:” den sonraki sayısal değer **CUSTOMINT1**’e ve **EVENTCATEGORY** kısmınıda “System” yazılacak.

Mesajta “User Accounts modified” ve varsa:

Kırmızı yazılı ifade **CUSTOMSTR1**’e ve **EVENTCATEGORY** kısmınıda “Login” yazılacak.

* ifadenin akabindeki “ Removed ” ifadesi **CUSTOMINT4**’e yazılacak.
* ifadenin akabindeki “ Added ” ifadesi **CUSTOMINT4**’e yazılacak.

Mesajta “Login succeeded” varsa:

Kırmızı yazılı ifade **CUSTOMSTR1**’e ve **EVENTCATEGORY** kısmınıda “Login” yazılacak.

Mesajta “Login failed” varsa:

Kırmızı yazılı ifade **CUSTOMSTR1**’e ve **EVENTCATEGORY** kısmınıda “Login” yazılacak.

* ifadenin akabindeki “ Reaseon ” ifadesinin karşısındaki değer **CUSTOMINT6**’e yazılacak.

Mesajta “Session timed out” varsa:

Kırmızı yazılı ifade **CUSTOMSTR1**’e ve **EVENTCATEGORY** kısmınıda “Logout” yazılacak.

* ifadenin akabindeki “ last access at ” ifadesinin karşısındaki tarih bilgisi **CUSTOMINT8**’e yazılacak.

Örn: ( last access at 17:55:09 2002/04/07 )

Mesajta “WebRequest ok” varsa:

Kırmızı yazılı ifade **CUSTOMSTR1**’e ve **EVENTCATEGORY** kısmınıda “WebRequest” yazılacak.

* ifadenin akabindeki “ Host ” ifadesi sonrasındaki IP adres **CUSTOMINT7**’e yazılacak.
* ifadenin akabindeki “ GET / POST ” ifadesi içeren istek türü **CUSTOMINT9**’e yazılacak.
* URL adresi bilgisi **CUSTOMINT10**’e yazılacak.

Mesajta “WebRequest completed” varsa:

Kırmızı yazılı ifade **CUSTOMSTR1**’e ve **EVENTCATEGORY** kısmınıda “WebRequest” yazılacak.

* ifadenin akabindeki “ from ” ifadesi sonrasındaki IP adres **CUSTOMINT7**’e yazılacak.
* ifadenin akabindeki “ GET / POST ” ifadesi içeren istek türü **CUSTOMINT9**’e yazılacak.
* URL adresi bilgisi **CUSTOMINT10**’e yazılacak.