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 | Cisco 6509 Switch |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | Cisco6500SyslogRecorder |
| 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 |  |

# ÖRNEK PARSING 1

|  |  |
| --- | --- |
| **10.101.30.1:514 : local7.notice :Feb 08 14:28:57 GMT: %FWSM-session-5-304001: 10.100.70.37 Accessed URL 85.111.6.19:/mesajlar/yenimesajkontrol?\_=1360326537266** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | DATETIME NOW |
| SOURCENAME | **notice** |
| EVENTCATEGORY |  |
| EVENTTYPE | **Accessed URL** |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | **10.101.30.1:514** |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **10.100.70.37** |
| CUSTOMSTR4 | **85.111.6.19** |
| CUSTOMSTR5 | **/mesajlar/yenimesajkontrol?\_=1360326537266 900 kontrolü yapılacak.** |
| CUSTOMSTR6 | 900 aşmasında kalan veri bu alana basılacak. 900 kontrolü eklenmesinde fayda var |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | FULL LOG |

# ÖRNEK PARSING 2

|  |  |
| --- | --- |
| **10.101.30.1:514 : local7.debug :Feb 08 14:31:15 GMT: %FWSM-session-7-106100: access-list vlan\_GUVENLI-DMZ\_out permitted udp inside\_SSG-550/192.168.20.27(49418) -> vlan\_GUVENLI-DMZ/SERVER\_DC-NEPTUN1\_10.101.30.249(53) hit-cnt 1 (first hit) [0x3e9992e1, 0x0]** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | DATETIME NOW |
| SOURCENAME | **debug** |
| EVENTCATEGORY | **access-list** |
| EVENTTYPE | **udp** |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | **10.101.30.1:514** |
| CUSTOMSTR1 | **vlan\_GUVENLI-DMZ\_out** |
| CUSTOMSTR2 | **inside\_SSG-550** |
| CUSTOMSTR3 | **192.168.20.27** |
| CUSTOMSTR4 | **SERVER\_DC-NEPTUN1\_10.101.30.249** |
| CUSTOMSTR5 | **vlan\_GUVENLI-DMZ** |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | **49418** |
| CUSTOMINT4 | **53** |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | FULL LOG |

# ÖRNEK PARSING 3

|  |  |
| --- | --- |
| **10.101.30.1:514 : local7.warning :Feb 08 14:31:15 GMT: %FWSM-session-4-106023: Deny udp src vlan\_ILO-BLADE:10.101.41.100/58660 dst vlan\_GUVENLI-DMZ:SERVER\_DC-NEPTUN2\_10.101.30.250/53 by access-group "vlan\_ILO-BLADE\_access\_in" [0x0, 0x0]** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | DATETIME NOW |
| SOURCENAME | **warning** |
| EVENTCATEGORY | **Deny** |
| EVENTTYPE | **udp** |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | **10.101.30.1:514** |
| CUSTOMSTR1 | **vlan\_ILO-BLADE\_access\_in** |
| CUSTOMSTR2 | **vlan\_ILO-BLADE** |
| CUSTOMSTR3 | **10.101.41.100** |
| CUSTOMSTR4 | **SERVER\_DC-NEPTUN2\_10.101.30.250** |
| CUSTOMSTR5 | **vlan\_GUVENLI-DMZ** |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | **58660** |
| CUSTOMINT4 | **53** |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | FULL LOG |

# ÖRNEK PARSING 4

|  |  |
| --- | --- |
| **10.101.30.1:514 : local7.error :Feb 08 15:31:23 GMT: %FWSM-ip-3-313001: Denied ICMP type=8, code=0 from 10.100.254.10 on interface vlan\_e-DevletDEV** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | DATETIME NOW |
| SOURCENAME | **error** |
| EVENTCATEGORY | **Denied** |
| EVENTTYPE | **ICMP** |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | **10.101.30.1:514** |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 | **vlan\_e-DevletDEV** |
| CUSTOMSTR3 | **10.100.254.10** |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | FULL LOG |

# ÖRNEK PARSING 5

|  |  |
| --- | --- |
| **10.101.30.1:514 : local7.error :Feb 08 15:31:19 GMT: %FWSM-session-3-710003: tcp access denied by ACL from 10.100.10.128/63355 to vlan\_PERSONEL:10.100.8.1/80** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | DATETIME NOW |
| SOURCENAME | **error** |
| EVENTCATEGORY | **denied** |
| EVENTTYPE | **tcp access** |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | **10.101.30.1:514** |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **10.100.10.128** |
| CUSTOMSTR4 | **10.100.8.1** |
| CUSTOMSTR5 | **vlan\_PERSONEL** |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | **63355** |
| CUSTOMINT4 | **80** |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | FULL LOG |

# 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 |  |