İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc330026386)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc330026387)

[ÖRNEK PARSING I 4](#_Toc330026388)

[ÖRNEK PARSING II 6](#_Toc330026389)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
| 02.09.2013 | V1 | Microsoft NPS | Kaan Emre KOŞAR |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | - |
| Ürün Adı | Microsoft NPS |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | C:\LOGS\MicrosoftNPS |
| İstek yapan Adı Soyadı | Kaan Emre KOŞAR |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 02.09.2013 |
| İstek yapılan kurum adı | Çalışma ve Sosyal Güvenlik Bakanlığı |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | C:\Windows\System32\LogFiles\IN130902.log |
| İlişkili form adı |  |
| Servis Yetkilisi Notları | Okunacak log dosyası adı rol ayarının günlük veya aylık olarak yapılmasına göre değişmektedir.  Örn1: IN130902.log, IN130903.log (günlük)  Örn2: IN1309.log, IN1310.log (aylık)  Okunacak iki farklı satır log tipi mevcuttur. Bu tiplerin haricindeki satırlar olduğu gibi descriptiona basılacaktır. |
| Geliştirici Notları |  |

# ÖRNEK PARSING-I

|  |  |
| --- | --- |
| <Event><Timestamp data\_type="4">09/02/2013 09:28:31.755</Timestamp><Computer-Name data\_type="1">SP000NPS01</Computer-Name><Event-Source data\_type="1">IAS</Event-Source><User-Name data\_type="1">gcetin</User-Name><Calling-Station-Id data\_type="1">88-c6-63-d2-66-95</Calling-Station-Id><Called-Station-Id data\_type="1">54-78-1a-21-0d-10:CSGB-Personel</Called-Station-Id><NAS-Port data\_type="0">13</NAS-Port><NAS-IP-Address data\_type="3">10.100.1.30</NAS-IP-Address><NAS-Identifier data\_type="1">WLC-01</NAS-Identifier><Vendor-Specific data\_type="2">00003763010600000002</Vendor-Specific><Service-Type data\_type="0">2</Service-Type><Framed-MTU data\_type="0">1300</Framed-MTU><NAS-Port-Type data\_type="0">19</NAS-Port-Type><Tunnel-Type data\_type="0">13</Tunnel-Type><Tunnel-Medium-Type data\_type="0">6</Tunnel-Medium-Type><Tunnel-Pvt-Group-ID data\_type="1">230</Tunnel-Pvt-Group-ID><Client-IP-Address data\_type="3">10.100.1.30</Client-IP-Address><Client-Vendor data\_type="0">0</Client-Vendor><Client-Friendly-Name data\_type="1">Cisco-WLC</Client-Friendly-Name><Cisco-AV-Pair data\_type="1">audit-session-id=0a64011e000025ab522423f8</Cisco-AV-Pair><Proxy-Policy-Name data\_type="1">Use Windows authentication for all users</Proxy-Policy-Name><Provider-Type data\_type="0">1</Provider-Type><SAM-Account-Name data\_type="1">CALISMA\gcetin</SAM-Account-Name><Class data\_type="1">311 1 10.0.200.226 08/16/2013 11:08:22 175448</Class><Fully-Qualifed-User-Name data\_type="1">calisma.local/CSGB/000/Users/Gizem Çetin</Fully-Qualifed-User-Name><Authentication-Type data\_type="0">5</Authentication-Type><NP-Policy-Name data\_type="1">WLC-01</NP-Policy-Name><Quarantine-Update-Non-Compliant data\_type="0">0</Quarantine-Update-Non-Compliant><Packet-Type data\_type="0">1</Packet-Type><Reason-Code data\_type="0">0</Reason-Code></Event> | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 09/02/2013 09:28:31.755 |
| SOURCENAME | CSGB-Personel |
| EVENTCATEGORY |  |
| EVENTTYPE | Cisco-WLC |
| USERSID | gcetin |
| LOGNAME | (Recorder Adı) |
| COMPUTERNAME | SP000NPS01 |
| CUSTOMSTR1 | 88-c6-63-d2-66-95 |
| CUSTOMSTR2 | CALISMA\gcetin |
| CUSTOMSTR3 | 10.100.1.30 |
| CUSTOMSTR4 | calisma.local/CSGB/000/Users/ |
| CUSTOMSTR5 | Gizem Çetin |
| CUSTOMSTR6 | 54-78-1a-21-0d-10 |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 | 10.100.1.30 |
| CUSTOMINT1 | 19 |
| CUSTOMINT2 | 13 |
| CUSTOMINT3 | 1 |
| CUSTOMINT4 | 5 |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Tüm log |

# 

# ÖRNEK PARSING-II

|  |  |
| --- | --- |
| <Event><Timestamp data\_type="4">09/01/2013 00:08:05.295</Timestamp><Computer-Name data\_type="1"> SP000NPS01</Computer-Name><Event-Source data\_type="1">IAS</Event-Source><User-Name data\_type="1">netadmin</User-Name><NAS-Port-Type data\_type="0">5</NAS-Port-Type><NAS-Port data\_type="0">0</NAS-Port><Acct-Status-Type data\_type="0">2</Acct-Status-Type><Acct-Session-Id data\_type="1">10.0.200.150@ssh.25037</Acct-Session-Id><Acct-Authentic data\_type="0">1</Acct-Authentic><NAS-IP-Address data\_type="3">10.0.200.253</NAS-IP-Address><Client-IP-Address data\_type="3">10.0.200.253</Client-IP-Address><Client-Vendor data\_type="0">9</Client-Vendor><Client-Friendly-Name data\_type="1">N7009-02</Client-Friendly-Name><Cisco-AV-Pair data\_type="1">accounting:accountinginfo=</Cisco-AV-Pair><Proxy-Policy-Name data\_type="1">Use Windows authentication for all users</Proxy-Policy-Name><Packet-Type data\_type="0">4</Packet-Type><Reason-Code data\_type="0">0</Reason-Code></Event> | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 09/01/2013 00:08:05.295 |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE | N7009-02 |
| USERSID | netadmin |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | 10.0.200.253 |
| CUSTOMSTR4 | 10.0.200.150@ssh.25037 |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 | 10.0.200.253 |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | 4 |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Tüm log |