İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc330026386)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc330026387)

[ÖRNEK PARSING 4](#_Toc330026388)

[TEMEL PARSING YAPISI 5](#_Toc330026389)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
| 23.07.2012 | V1 | 2008 Türkçe Logların Alınması | Hüseyin Sevin |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | - |
| Ürün Adı | WindowsServer2008Türkçe DC Eventlog |
| Versiyonu | 2008 |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | NtEventLog2008TRV1\_1\_1\_Recorder |
| İstek yapan Adı Soyadı | Hüseyin Sevin |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 23.07.2012 |
| İstek yapılan kurum adı | Tigem |
| 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

|  |  |
| --- | --- |
| Ağ paylaşım nesnesi istemcinin istenen erişimi sağlayıp sağlamadığını görmek için kontrol edildi. Nesne: Güvenlik Kimliği: S-1-5-18 Hesap Adı: TIGEMAD$ Hesap Etki Alanı: TIGEM Oturum Açma Kimliği: 0x36abc07 Ağ Bilgileri: Nesne Türü: File Kaynak Adresi: ::1 Kaynak Bağlantı Noktası: 50768 Paylaşım Bilgileri: Paylaşım Adı: \\\*\SYSVOL Paylaşım Yolu: \??\C:\Windows\SYSVOL\sysvol Göreli Hedef Adı: Erişim İsteği Bilgileri: Erişim Maskesi: 0x100080 Erişimler: SYNCHRONIZE ReadAttributes Erişim Kontrolü Sonuçları: SYNCHRONIZE: Yetki veren D:(A;;0x1200a9;;;WD) ReadAttributes: Yetki veren D:(A;;0x1200a9;;;WD) | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | TimeGenerated |
| SOURCENAME | SourceName |
| EVENTCATEGORY | CategoryString |
| EVENTTYPE | Type |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | ComputerName |
| CUSTOMSTR1 | Hesap Adı |
| CUSTOMSTR2 | Paylaşım Adı |
| CUSTOMSTR3 | Kaynak Adresi |
| CUSTOMSTR4 | - |
| CUSTOMSTR5 | Hesap Etki Alanı |
| CUSTOMSTR6 | Oturum Açma Kimliği |
| CUSTOMSTR7 | - |
| CUSTOMSTR8 | Remote\_host |
| CUSTOMSTR9 | - |
| CUSTOMSTR10 | - |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 | Kaynak Bağlantı Noktası |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 | RecordNumber |
| DESCRIPTION | Tam 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 |  |