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 |
| 10.01.2013 | v.1.0.2 | Nps 2008 (radius) loglarının alınması | Emre BAŞTUĞ |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | Microsoft Network Policy and Access Services |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | NPS2008V\_1\_0\_0Recorder |
| İstek yapan Adı Soyadı | Emre BAŞTUĞ |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 09.01.2013 |
| İstek yapılan kurum adı | Exim Bank |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | C:\Windows\System32\LogFiles\IN(ay bilgisi).log (loglar aylık olarak rotate olmaktadır) |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları |  |

**ÖRNEK PARSING (1) (tamamlandı)**

|  |  |
| --- | --- |
| **"DHCPRAD","IAS",12/25/2012,09:38:41,1,"hb1029","EXIMBANK\hb1029","C4-01-7C-FC-43-F8:tisya","24-AB-81-83-89-3C",,,"C4-01-7C-FC-43-F8","172.16.110.254",2,0,"172.16.110.254","Ruckus1100",,,19,"CONNECT 802.11g/n",,2,,,0,"311 1 ::1 12/24/2012 19:04:51 1533",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"ruckus",1,,,,**  **"DHCPRAD","IAS",12/25/2012,09:38:41,11,,"EXIMBANK\hb1029",,,,,,,,0,"172.16.110.254","Ruckus1100",,,,,,,,,0,"311 1 ::1 12/24/2012 19:04:51 1533",30,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"ruckus",1,,,,** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **12/25/2012,09:38:41** |
| SOURCENAME | **ruckus** |
| EVENTCATEGORY | **IAS** |
| EVENTTYPE | **CONNECT** |
| USERSID | **hb1029** |
| LOGNAME |  |
| COMPUTERNAME | **C4-01-7C-FC-43-F8** |
| CUSTOMSTR1 | **Ruckus1100** |
| CUSTOMSTR2 | **tisya** |
| CUSTOMSTR3 | **172.16.110.254** |
| CUSTOMSTR4 | **DHCPRAD** |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 | **24-AB-81-83-89-3C** |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 | **802.11g/n** |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

# ÖRNEK PARSING (2) (customstr2 deki user, customstr5 e alınacak)

|  |  |
| --- | --- |
| **"DHCPRAD","IAS",12/25/2012,09:38:41,11,,"EXIMBANK\hb1029",,,,,,,,0,"172.16.110.254","Ruckus1100",,,,,,,,,0,"311 1 ::1 12/24/2012 19:04:51 1533",30,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"ruckus",1,,,,** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **12/25/2012,09:38:41** |
| SOURCENAME | **ruckus** |
| EVENTCATEGORY | **IAS** |
| EVENTTYPE |  |
| USERSID | **hb1029** |
| LOGNAME |  |
| COMPUTERNAME | **C4-01-7C-FC-43-F8** |
| CUSTOMSTR1 | **Ruckus1100** |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **172.16.110.254** |
| CUSTOMSTR4 | **DHCPRAD** |
| CUSTOMSTR5 | **EXIMBANK\ hb1029** |
| CUSTOMSTR6 | **24-AB-81-83-89-3C** |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 | **802.11g/n** |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

# ÖRNEK PARSING (3)

|  |  |
| --- | --- |
| "**DHCPRAD**","**IAS"**,**11/01/2012,08:16:48,11**,,"eximbank.ic/EximComputers/**SIG\_EY1247**",,,,,,,,0,"**172.16.110.254**","**Ruckus1100**",**,,,,,,11**,"**Connections to other access servers**",**0,"311 1** **::1** **09/25/2012 07:14:34** **119817**",**30**,**,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,**"**ruckus**"**,1,,,,** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **12/25/2012,09:38:41** |
| SOURCENAME | **ruckus** |
| EVENTCATEGORY | **IAS** |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | **Ruckus1100** |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **172.16.110.254** |
| CUSTOMSTR4 | **DHCPRAD** |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 | **SIG\_EY1247** |
| CUSTOMSTR10 | **Connections to other access servers** |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME | *Log Time* |
| SOURCENAME | ProxyPolicyName |
| EVENTCATEGORY | EventCategory |
| EVENTTYPE | Connection status |
| USERSID | SubjectUserName |
| LOGNAME |  |
| COMPUTERNAME | Client Machine MAC |
| CUSTOMSTR1 | RadiusClient Name |
| CUSTOMSTR2 | Called Station Identifier |
| CUSTOMSTR3 | RADIUS Client IP Address |
| CUSTOMSTR4 | Authentication Server |
| CUSTOMSTR5 | Domain\Username |
| CUSTOMSTR6 | Radius MAC |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 | WLAN Type |
| CUSTOMSTR9 | COMPUTERNAME |
| CUSTOMSTR10 | Connection Description |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full log |

NETWORK POLICY AND ACCESS SERVICES XML FORMATI

|  |
| --- |
| XML IMFORMATİON |
| - <Event xmlns="<http://schemas.microsoft.com/win/2004/08/events/event>">  - <System>  <Provider Name="**Microsoft-Windows-Security-Auditing**" Guid="**{54849625-5478-4994-a5ba-3e3b0328c30d}**" />  <EventID>6272</EventID>  <Version>0</Version>  <Level>0</Level>  <Task>12552</Task>  <Opcode>0</Opcode>  <Keywords>0x8020000000000000</Keywords>  <TimeCreated SystemTime="**2012-12-25T09:27:13.419Z**" />  <EventRecordID>17817789</EventRecordID>  <Correlation />  <Execution ProcessID="**664**" ThreadID="**3644**" />  <Channel>Security</Channel>  <Computer>DHCPRAD.eximbank.ic</Computer>  <Security />  </System>  - <EventData>  <Data Name="**SubjectUserSid**">S-1-5-21-749490177-939355003-1232828436-1036</Data>  <Data Name="**SubjectUserName**">am441</Data>  <Data Name="**SubjectDomainName**">EXIMBANK</Data>  <Data Name="**FullyQualifiedSubjectUserName**">eximbank.ic/Users/Alaaddin METİN</Data>  <Data Name="**SubjectMachineSID**">S-1-0-0</Data>  <Data Name="**SubjectMachineName**">-</Data>  <Data Name="**FullyQualifiedSubjectMachineName**">-</Data>  <Data Name="**MachineInventory**">-</Data>  <Data Name="**CalledStationID**">C4-01-7C-FC-43-68:tisya</Data>  <Data Name="**CallingStationID**">34-51-C9-B5-2A-9A</Data>  <Data Name="**NASIPv4Address**">172.16.110.254</Data>  <Data Name="**NASIPv6Address**">-</Data>  <Data Name="**NASIdentifier**">C4-01-7C-FD-43-68</Data>  <Data Name="**NASPortType**">Wireless - IEEE 802.11</Data>  <Data Name="**NASPort**">1</Data>  <Data Name="**ClientName**">Ruckus100</Data>  <Data Name="**ClientIPAddress**">172.16.110.223</Data>  <Data Name="**ProxyPolicyName**">ruckus</Data>  <Data Name="**NetworkPolicyName**">WLANNUMBER</Data>  <Data Name="**AuthenticationProvider**">Windows</Data>  <Data Name="**AuthenticationServer**">DHCPRAD.eximbank.ic</Data>  <Data Name="**AuthenticationType**">PEAP</Data>  <Data Name="**EAPType**">Microsoft: Secured password (EAP-MSCHAP v2)</Data>  <Data Name="**AccountSessionIdentifier**">-</Data>  <Data Name="**QuarantineState**">Full Access</Data>  <Data Name="**QuarantineSessionIdentifier**">-</Data>  </EventData>  </Event> |

ERROR LOG XML FORMATI

NETWORK POLICY SERVİCES ERROR LOGU XML FORMATI

|  |  |
| --- | --- |
| XML ERROR |  |
| <Event xmlns="<http://schemas.microsoft.com/win/2004/08/events/event>">  - <System>  <Provider Name="**NPS**" />  <EventID Qualifiers="**49152**">4402</EventID>  <Level>2</Level>  <Task>0</Task>  <Keywords>0x80000000000000</Keywords>  <TimeCreated SystemTime="**2012-12-25T08:54:23.000Z**" />  <EventRecordID>629529</EventRecordID>  <Channel>System</Channel>  <Computer>DHCPRAD.eximbank.ic</Computer>  <Security />  </System>  - <EventData>  <Data>DENETCI1</Data>  </EventData>  </Event> | <Event xmlns="<http://schemas.microsoft.com/win/2004/08/events/event>">  - <System>  <Provider Name="**NPS**" />  <EventID Qualifiers="**49152**">13</EventID>  <Level>2</Level>  <Task>0</Task>  <Keywords>0x80000000000000</Keywords>  <TimeCreated SystemTime="**2012-12-22T14:14:58.000Z**" />  <EventRecordID>628905</EventRecordID>  <Channel>System</Channel>  <Computer>DHCPRAD.eximbank.ic</Computer>  <Security />  </System>  - <EventData>  <Data>172.16.254.254</Data>  </EventData>  </Event> |