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 |
| 24.05.2013 | 2.0 | ArubaSyslog | Deniz Aksoy |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | 01 |
| Ürün Adı | ZimbraMail |
| Versiyonu | 2.0 |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi |  |
| İstek yapan Adı Soyadı | Deniz Aksoy |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 24.05.2013 |
| İstek yapılan kurum adı | Kafkas Üniversitesi |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | UDP :514 |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları |  |

# 

# PARSING User Authentication Successful

|  |  |
| --- | --- |
| 10.1.5.10:514 : local7.notice May 6 17:34:06 THK-650 authmgr[1589]: <522008> <NOTI> <THK-650 10.1.5.10> User Authentication Successful: username=agencses MAC=00:23:6c:2e:96:84 IP=10.2.129.72 role=Personel-Role VLAN=231 AP=THKU REKTORLUK 1.KAT-5 SSID=THKU-802.1x AAA profile=THK-PERSONEL-802.1X-AAA-Profile auth method=802.1x auth server=THK-RADIUS-Server | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | May 6 17:34:06 |
| SOURCENAME | THK-650 |
| EVENT ID |  |
| EVENTCATEGORY | User Authentication Successful |
| EVENTTYPE | local7.notice |
| USERSID | username=agencses |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | MAC=00:23:6c:2e:96:84 |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | IP=10.2.129.72 |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 | role=Personel-Role |
| CUSTOMSTR7 | profile=THK-PERSONEL |
| CUSTOMSTR8 | VLAN=231 |
| CUSTOMSTR9 | AP=THKU REKTORLUK 1.KAT-5 |
| CUSTOMSTR10 | server=THK-RADIUS-Server |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | 10.1.5.10 |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 10.1.5.10:514 : local7.notice May 6 17:34:06 THK-650 authmgr[1589]: <522008> <NOTI> <THK-650 10.1.5.10> User Authentication Successful: username=agencses MAC=00:23:6c:2e:96:84 IP=10.2.129.72 role=Personel-Role VLAN=231 AP=THKU REKTORLUK 1.KAT-5 SSID=THKU-802.1x AAA profile=THK-PERSONEL-802.1X-AAA-Profile auth method=802.1x auth server=THK-RADIUS-Server |

# 

# PARSING User Authentication Failed

|  |  |
| --- | --- |
| 10.1.5.10:514 : local7.notice May 6 17:46:19 THK-650 authmgr[1589]: <522042> <NOTI> <THK-650 10.1.5.10> User Authentication Failed: username=yeliz\_ozyilmaz@hotmail.com MAC=64:a7:69:e9:6f:0d IP=0.0.0.0 auth method=802.1x auth server=THK-RADIUS-Server | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | May 6 17:46:19 |
| SOURCENAME | THK-650 |
| EVENT ID |  |
| EVENTCATEGORY | User Authentication Failed |
| EVENTTYPE | local7.notice |
| USERSID | username=yeliz\_ozyilmaz@hotmail.com |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | MAC=64:a7:69:e9:6f:0d |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | IP=0.0.0.0 |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 | server=THK-RADIUS-Server |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | 10.1.5.10 |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 10.1.5.10:514 : local7.notice May 6 17:46:19 THK-650 authmgr[1589]: <522042> <NOTI> <THK-650 10.1.5.10> User Authentication Failed: username=yeliz\_ozyilmaz@hotmail.com MAC=64:a7:69:e9:6f:0d IP=0.0.0.0 auth method=802.1x auth server=THK-RADIUS-Server |

# PARSING Adding user

|  |  |
| --- | --- |
| 10.1.5.10:514 : local7.debug May 6 17:47:02 THK-650 authmgr[1589]: <522004> <DBUG> <THK-650 10.1.5.10> icmp request sent for user 10.2.129.72  10.1.5.10:514 : local7.debug May 6 17:47:02 THK-650 authmgr[1589]: <121031> <DBUG> <THK-650 10.1.5.10> |aaa| [rc\_sequence.c:107] seq\_num\_timeout\_handler: Freed 0 entries  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <124004> <DBUG> <THK-650 10.1.5.10> Free ipuser 0x0x1095ee5c (10.2.129.37) for user 0x0x1092ddcc  10.1.5.10:514 : local7.info May 6 17:46:59 THK-650 authmgr[1589]: <522050> <INFO> <THK-650 10.1.5.10> MAC=34:51:c9:5b:b8:47,IP=N/A User data downloaded to datapath, new Role=Personel-Role/55, bw Contract=0/0,reason=Station resetting role  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <124004> <DBUG> <THK-650 10.1.5.10> Tx message to Sibyte, blocking with ack. Opcode = 17, msglen = 192 action = 17  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <522004> <DBUG> <THK-650 10.1.5.10> download-L2: acl=55/0 role=Personel-Role, tunl=0x1110, PA=0, HA=1, RO=0, VPN=0  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <124004> <DBUG> <THK-650 10.1.5.10> Adding user: 1092ddcc (34:51:c9:5b:b8:47:N/A:eakant) to ap group:THK-AP-Group ap group id: 3737 role:Personel-Role  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <522004> <DBUG> <THK-650 10.1.5.10> MAC=34:51:c9:5b:b8:47 Reset station role to Personel-Role (55) (ingress=4368)  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <124004> <DBUG> <THK-650 10.1.5.10> sta\_del\_l3: mac 34:51:c9:5b:b8:47 ip 10.2.129.37  10.1.5.10:514 : local7.info May 6 17:46:59 THK-650 authmgr[1589]: <522005> <INFO> <THK-650 10.1.5.10> MAC=34:51:c9:5b:b8:47 IP=10.2.129.37 User entry deleted: reason=idle timeout  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <124004> <DBUG> <THK-650 10.1.5.10> MM: mac=34:51:c9:5b:b8:47, state=2, name=eakant, role=Personel-Role, dev\_type=iPad, ip=10.2.129.37  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <124004> <DBUG> <THK-650 10.1.5.10> Tx message to Sibyte, blocking with ack. Opcode = 17, msglen = 192 action = 1  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <522004> <DBUG> <THK-650 10.1.5.10> {10.2.129.37} datapath entry deleted  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <124004> <DBUG> <THK-650 10.1.5.10> Tx message to Sibyte, blocking with ack. Opcode = 17, msglen = 192 action = 5  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <522004> <DBUG> <THK-650 10.1.5.10> MAC=34:51:c9:5b:b8:47 IP=10.2.129.37 Send mobility delete message, flags=0x0  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <522004> <DBUG> <THK-650 10.1.5.10> AU1(4), HA1, TAP0, PARP0 OIP0 IIP0 INT0 WD0 FW0 DT1  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <124004> <DBUG> <THK-650 10.1.5.10> AP-GROUP:3736 Group Name: THK-AP-Group released  10.1.5.10:514 : local7.debug May 6 17:46:59 THK-650 authmgr[1589]: <522004> <DBUG> <THK-650 10.1.5.10> User idle ip=10.2.129.37, role=Personel-Role  10.1.5.10:514 : local7.debug May 6 17:46:54 THK-650 authmgr[1589]: <522004> <DBUG> <THK-650 10.1.5.10> MAC=34:51:c9:5b:b8:47 IP=10.2.129.37 Sending ping 3 of 3 (id=8214, seq=29898)  10.1.5.10:514 : local7.debug May 6 17:46:54 THK-650 authmgr[1589]: <522004> <DBUG> <THK-650 10.1.5.10> icmp request sent for user 10.2.129.37  10.1.5.10:514 : local7.debug May 6 17:46:49 THK-650 authmgr[1589]: <522004> <DBUG> <THK-650 10.1.5.10> MAC=34:51:c9:5b:b8:47 IP=10.2.129.37 Sending ping 2 of 3 (id=8214, seq=29897)  10.1.5.10:514 : local7.debug May 6 17:46:49 THK-650 authmgr[1589]: <522004> <DBUG> <THK-650 10.1.5.10> icmp request sent for user 10.2.129.37  10.1.5.10:514 : local7.debug May 6 17:46:48 THK-650 authmgr[1589]: <121031> <DBUG> <THK-650 10.1.5.10> |aaa| [rc\_sequence.c:107] seq\_num\_timeout\_handler: Freed 0 entries  10.1.5.10:514 : local7.debug May 6 17:46:44 THK-650 authmgr[1589]: <522004> <DBUG> <THK-650 10.1.5.10> MAC=34:51:c9:5b:b8:47 IP=10.2.129.37 Sending ping 1 of 3 (id=8214, seq=29896)  10.1.5.10:514 : local7.debug May 6 17:46:44 THK-650 authmgr[1589]: <522004> <DBUG> <THK-650 10.1.5.10> icmp request sent for user 10.2.129.37 | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | May 6 17:46:49 |
| SOURCENAME | THK-650 |
| EVENT ID |  |
| EVENTCATEGORY | Adding user |
| EVENTTYPE | local7.debug |
| USERSID | name=eakant |
| LOGNAME |  |
| COMPUTERNAME | dev\_type=iPad |
| CUSTOMSTR1 | MAC=34:51:c9:5b:b8:47 |
| CUSTOMSTR2 | Group Name: THK-AP-Group |
| CUSTOMSTR3 | IP=10.2.129.37 |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 | role=Personel-Role |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | 10.1.5.10 |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | May 7 11:52:02 mail postfix/qmgr[23718]: 7E46A1A3D915: from=<gurun@kafkas.edu.tr>, size=2477103, nrcpt=1 (queue active)  May 7 11:52:02 mail postfix/smtp[10677]: 9F39A1A3DA55: to=<suleymanerarslan@hotmail.com>, relay=127.0.0.1[127.0.0.1]:10024, delay=0.94, delays=0.15/0/0/0.79, dsn=2.0.0, status=sent (250 2.0.0 from MTA([127.0.0.1]:10025): 250 2.0.0 Ok: queued as 7E46A1A3D915) |

# PARSING Attack

|  |  |
| --- | --- |
| 10.1.5.10:514 : local7.warning May 6 17:44:06 THK-650 wms[1580]: <126087> <WARN> <THK-650 10.1.5.10> |ids| AP(6c:f3:7f:13:a5:30@THKU FAKULTE B-BLOK KAT1-8): Block ACK DoS Attack: An AP detected a data frame which indicates a possible Block ACK DoS Attack. The frame from cc:cc:81:39:55:4b to 74:2f:68:49:61:cd (BSSID 6c:f3:7f:13:a0:43 on CHANNEL 6 with SNR 18) is outside the current sequence number window, and thus may be dropped. Associated WVE ID(s): WVE-2008-0006. | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | May 6 17:34:06 |
| SOURCENAME | THK-650 |
| EVENT ID |  |
| EVENTCATEGORY | Block ACK DoS Attack |
| EVENTTYPE | local7.warning |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | 6c:f3:7f:13:a5:30@THKU FAKULTE B-BLOK KAT1-8 |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 |  |
| CUSTOMSTR4 | from cc:cc:81:39:55:4b |
| CUSTOMSTR5 | to 74:2f:68:49:61:cd |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | 10.1.5.10 |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 10.1.5.10:514 : local7.warning May 6 17:45:36 THK-650 wms[1580]: <126087> <WARN> <THK-650 10.1.5.10> |ids| AP(6c:f3:7f:13:a7:b0@THKU FAKULTE B-BLOK KAT1-9): Block ACK DoS Attack: An AP detected a data frame which indicates a possible Block ACK DoS Attack. The frame from cc:cc:81:39:55:4b to 74:2f:68:49:61:cd (BSSID 6c:f3:7f:13:a0:43 on CHANNEL 6 with SNR 21) is outside the current sequence number window, and thus may be dropped. Associated WVE ID(s): WVE-2008-0006. |

# PARSING Dhcp

|  |  |
| --- | --- |
| 10.1.5.10:514 : local7.debug May 30 10:25:01 THK-650 authmgr[1585]: <522004> <DBUG> <THK-650 10.1.5.10> DHCP ACK mac 5c:0a:5b:2b:25:59, client ip 10.2.160.71, server ip 0.0.0.0  10.1.5.10:514 : local7.debug May 30 10:24:59 THK-650 authmgr[1585]: <522004> <DBUG> <THK-650 10.1.5.10> DHCP ACK mac a4:17:31:87:9a:87, client ip 10.2.128.159, server ip 0.0.0.0  10.1.5.10:514 : local7.debug May 30 10:24:58 THK-650 authmgr[1585]: <522004> <DBUG> <THK-650 10.1.5.10> DHCP ACK mac 34:c0:59:f3:1a:16, client ip 10.2.128.74, server ip 0.0.0.0  10.1.5.10:514 : local7.debug May 30 10:24:56 THK-650 authmgr[1585]: <522004> <DBUG> <THK-650 10.1.5.10> DHCP ACK mac a4:17:31:88:a2:d1, client ip 10.2.128.93, server ip 0.0.0.0  10.1.5.10:514 : local7.debug May 30 10:24:52 THK-650 authmgr[1585]: <522004> <DBUG> <THK-650 10.1.5.10> DHCP ACK mac 04:1e:64:73:ca:41, client ip 10.2.128.77, server ip 0.0.0.0  10.1.5.10:514 : local7.debug May 30 10:24:42 THK-650 authmgr[1585]: <522004> <DBUG> <THK-650 10.1.5.10> DHCP ACK mac a4:17:31:87:9a:87, client ip 10.2.128.159, server ip 0.0.0.0 | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | May 6 17:34:06 |
| SOURCENAME | THK-650 |
| EVENT ID |  |
| EVENTCATEGORY | DHCP |
| EVENTTYPE | local7.debug |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | mac a4:17:31:87:9a:87 |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | client ip 10.2.128.159 |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | 10.1.5.10 |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 10.1.5.10:514 : local7.debug May 30 10:25:04 THK-650 authmgr[1585]: <522004> <DBUG> <THK-650 10.1.5.10> DHCP ACK mac a4:17:31:87:dd:2f, client ip 10.2.128.138, server ip 0.0.0.0 |