

Router'in Syslog'u Toplamıyor

Syslog, sorun giderme için yararlı bilgiler sağlar. Syslog'u toplamının birkaç yolu vardır: Syslog Explorer, Syslog'u gözden geçirmek ve indirmek için hızlı bir yol sunarken, USB diskine kaydetme, Router'in daha fazla günlük tutmasına izin verir ve daha fazla bilgi içerir. Syslog Explorer veya USB Uygulamasını desteklemeyen bazı modellerde, Syslog'un tamamını toplamak için Syslog Yardımcı Programını([Syslog Utility](#)) kullanabiliriz.

Syslog Explorer Diagnostics >> Syslog Explorer'a gidin, **Enable Web Syslog'u** işaretleyin ve bir Syslog Type seçin; Router günlükleri kaydetmeye başlayacaktır. Syslog dosyasını kaydetmek için, lütfen **Export'a** tıklayın. Ardından, web_syslogxxxxxxx adlı bir dosya bilgisayarınıza indirilecektir, burada xxxxxxxx geçerli tarihtir.

Diagnostics >> Syslog Explorer

Web Syslog		USB Syslog	
<input checked="" type="checkbox"/>	Enable Web Syslog	Export Refresh Clear	
		Syslog Type	Display Mode
		Firewall ▼	Always record the new event ▼
Time	Message		
2015-02-06 06:43:17	[Pass][Unknown DNS query type][Hostname=]		
2015-02-06 05:46:21	[Pass][Unknown DNS query type][Hostname=]		
2015-02-06 05:26:59	[Pass][Unknown DNS query type][Hostname=]		
2015-02-06 04:06:51	[CSM_DNSF][Pass][@S:R=13:1, 192.168.1.10:1043->http://ads.yahoo.com:53][DNS][HLen=20, TLen=59]		
2015-02-06 04:05:41	[CSM_DNSF][Pass][@S:R=13:1, 192.168.1.10:1047->http://www.gstatic.com:53][DNS][HLen=20, TLen=61]		
2015-02-06 04:05:41	[CSM_DNSF][Pass][@S:R=13:1, 192.168.1.10:1043->http://apis.google.com:53][DNS][HLen=20, TLen=61]		
2015-02-06 04:05:41	[CSM_DNSF][Pass][@S:R=13:1, 192.168.1.10:1025->http://www.google.com:53][DNS][HLen=20, TLen=60]		
2015-02-06 04:05:41	[CSM_DNSF][Pass][@S:R=13:1, 192.168.1.10:3607->http://ssl.gstatic.com:53][DNS][HLen=20, TLen=61]		
2015-02-06 04:02:18	[CSM_DNSF][Pass][@S:R=13:1, 192.168.1.10:3607->http://clients4.google.com:53][DNS][HLen=20, TLen=65]		

Syslog'u USB Diske Kaydetme

1. Router'in USB bağlantı noktasına bir USB disk yerleştirin ve Router'in **USB Application >> USB Device Status** sayfası aracılığıyla algıladığını kontrol edin.

USB Application >> USB Device Status

Disk	Modem	Printer	Sensor	Refresh
USB Mass Storage Device Status				
Connection Status: Disk Connected				Disconnect USB Disk
Write Protect Status: No				
Disk Capacity: 3829 MB				
Free Capacity: 2705 MB Refresh				

2. USB Disk için Enable Syslog Access : **System Maintenance >> Syslog/Mail Alert Setup**'a gidin,

- Syslog Access Setup için Enable'yi işaretleyin
- USB Diski Syslog için kontrol edin
- Toplamak istediğiniz Syslog mesajlarını seçin
- Uygulamak için OK'a tıklayın.

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input type="checkbox"/> Syslog Server</p> <p><input checked="" type="checkbox"/> USB Disk</p> <p>Router Name DrayTek</p> <p>Server IP Address</p> <p>Destination Port 514</p> <p>Mail Syslog <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p>	<p>Mail Alert Setup</p> <p><input type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server</p> <p>SMTP Port 25</p> <p>Mail To</p> <p>Return-Path</p> <p><input type="checkbox"/> Use SSL</p> <p><input type="checkbox"/> Authentication</p> <p>Username</p> <p>Password</p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> APPE</p> <p><input checked="" type="checkbox"/> VPN LOG</p> <p><input type="checkbox"/> APPF Signature</p>
---	---

3. Günlükler hazır olduğunda, USB diskteki yeni bir Syslog klasörüne kaydedilirler. Dosyaları USB Application >> File Explorer'dan kontrol edebilir ve dosyayı çift tıklayarak bilgisayarınıza indirebilirsiniz.

USB Application >> File Explorer

File Explorer

Current Path: /

Name	Size	Delete	Rename
SysLog		X	
System Volume Information		X	

Sistem günlüğü Programı

Syslog Tool yüklü olan herhangi bir bilgisayar Syslog sunucusu olabilir. Değilse [Products > DrayTek Utility](#)'den indirebilirsiniz. Syslog Tool ile Syslog toplamak için lütfen aşağıdaki adımları gerçekleştirin:

- Router'da Syslog Access'i etkinleştirin: System Maintenance >> Syslog/Mail Alert Setup,'a gidin,
 - Syslog Erişim Kurulumu için Etkinleştir'i işaretleyin
 - Syslog için Syslog Server Seçin ve Kaydedin
 - Server IP Adresi için Syslog Tool'u çalıştıran bilgisayarın IP'sini girin.
 - Toplamak istediğiniz sistem günlüğü mesajlarını seçin.
 - Uygulamak için OK'a tıklayın.

SysLog / Mail Alert Setup

SysLog Access Setup <input checked="" type="checkbox"/> Enable Syslog Save to: <input checked="" type="checkbox"/> Syslog Server <input type="checkbox"/> USB Disk Router Name <input type="text"/> Server IP Address <input type="text" value="192.168.1.11"/> Destination Port <input type="text" value="514"/> Mail Syslog <input type="checkbox"/> Enable Enable syslog message: <input checked="" type="checkbox"/> Firewall Log <input checked="" type="checkbox"/> VPN Log <input checked="" type="checkbox"/> User Access Log <input checked="" type="checkbox"/> Call Log <input checked="" type="checkbox"/> WAN Log <input checked="" type="checkbox"/> Router/DSL information AlertLog Setup <input type="checkbox"/> Enable AlertLog Port <input type="text" value="514"/>		Mail Alert Setup <input type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/> SMTP Server <input type="text"/> SMTP Port <input type="text" value="25"/> Mail To <input type="text"/> Return-Path <input type="text"/> <input type="checkbox"/> Use SSL <input type="checkbox"/> Authentication Username <input type="text"/> Password <input type="text"/> Enable E-Mail Alert: <input checked="" type="checkbox"/> DoS Attack <input checked="" type="checkbox"/> IM-P2P <input checked="" type="checkbox"/> VPN LOG <input type="checkbox"/> APPE Signature
---	--	--

- Note:** 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".
 2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.
 3. We only support secured SMTP connection on port 465.

2. Bilgisayarda Syslog Tool'u çalıştırın. Sonra:

- Router'in LAN IP adresini seçin.
- WAN Interface'yi seçiniz.
- İhtiyaç duyduğunuz günlükleri topladıktan sonra, dosyayı kaydetmek için Save düğmes ine tıklayın.

Sorun Giderme: Yazılımda herhangi bir oturum açmadıysanız, lütfen **UDP port 514'ü** engelleyen bir kural olup olmadığını görmek için hem Router'deki hem de Syslog sunucusundaki (bilgisayar) firewall policy kontrol edin .

DrayTek Syslog Utility

c. **a.** 192.168.1.1 **b.** WAN2

Log Filter
Keyword:
Apply to: All Refresh

LAN Information
Vigor2860Vn
TX Packets: 29714 RX Packets: 32019

WAN Information
WAN IP (PPPoE): 118.160.93.121 Gateway IP (PPPoE): 168.95.98.254
TX Rate: 15 RX Rate: 28

Firewall VPN User Access Connection WAN IPBX Others

System Time	Router Time	Host	Message
2013-09-25 17:17:04	Sep 25 09:17:04	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:64016 -> 203.177.240.222:29012 (TCP)
2013-09-25 17:17:03	Sep 25 09:17:04	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:64015 -> 111.242.102.48:52515 (TCP)
2013-09-25 17:17:03	Sep 25 09:17:04	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:64015 -> 111.242.102.48:52515 (TCP)
2013-09-25 17:16:27	Sep 25 09:16:28	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:64017 -> 123.192.44.157:9369 (TCP)
2013-09-25 17:16:27	Sep 25 09:16:27	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:64017 -> 123.192.44.157:9369 (TCP)
2013-09-25 17:16:27	Sep 25 09:16:27	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:57015 -> 157.55.235.147:443 (UDP)
2013-09-25 17:16:27	Sep 25 09:16:27	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:57015 -> 157.55.130.169:443 (UDP)
2013-09-25 17:16:27	Sep 25 09:16:27	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:57015 -> 157.55.130.169:443 (UDP)
2013-09-25 17:16:27	Sep 25 09:16:27	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:64016 -> 203.177.240.222:29012 (TCP)
2013-09-25 17:16:27	Sep 25 09:16:27	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:64015 -> 111.242.102.48:52515 (TCP)
2013-09-25 17:16:27	Sep 25 09:16:27	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:57015 -> 92.83.54.107:15435 (UDP)
2013-09-25 17:16:27	Sep 25 09:16:27	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:57015 -> 82.65.183.39:49769 (UDP)
2013-09-25 17:16:27	Sep 25 09:16:27	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:57015 -> 76.88.174.159:63902 (UDP)
2013-09-25 17:16:27	Sep 25 09:16:27	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:57015 -> 75.54.22.129:34872 (UDP)
2013-09-25 17:16:15	Sep 25 09:16:16	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:57015 -> 157.56.52.30:40013 (UDP)
2013-09-25 17:14:19	Sep 25 09:14:19	Vigor	Local User: 74.125.31.102:443 -> 192.168.1.10:63992 (TCP) close connection
2013-09-25 17:14:19	Sep 25 09:14:19	Vigor	Local User: 74.125.31.190:443 -> 192.168.1.10:63991 (TCP) close connection
2013-09-25 17:13:38	Sep 25 09:13:38	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:57015 -> 64.4.23.159:40015 (UDP)
2013-09-25 17:13:36	Sep 25 09:13:37	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:57015 -> 157.55.56.143:40010 (UDP)
2013-09-25 17:13:31	Sep 25 09:13:31	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:63916 -> 157.56.194.8:443 (TCP) close
2013-09-25 17:13:31	Sep 25 09:13:31	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:64014 -> 157.56.194.8:443 (TCP)
2013-09-25 17:13:31	Sep 25 09:13:31	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:57015 -> 157.56.194.8:443 (TCP)
2013-09-25 17:13:31	Sep 25 09:13:31	Vigor	Local User (MAC=F8-1A-67-03-7F-59): 192.168.1.10:57015 -> 157.56.194.8:443 (TCP)

System Time: Time tag from the computer which runs the syslog application Router Time: Time tag from router

ADSL Status

Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att

3. Bir açılır pencere olacaktır. **Save current log to a file**'ı seçin, Log File name ve path(yol) girin ve kaydetmek için OK'a tıklayın.

Log Save

Save current log to a file
 Record log to a file in real time
 Record log to multiple files

Log File name: D:\User\Desktop\SyslogDB\log.1.log

Graph File name: (VPN Graph, Traffic Graph)

Auto launch Save to a file every: 1 Day(s)

Record Time Limit
 No Record Time Limit
 0 Day(s) 0 Hour(s) 0 Minute(s)

OK Cancel