آموزش ذخیره سازی لاگ میکروتیک

نویسنده رامین ملک قاسمی

Rmalekghasemi.ir

اهداف

ذخیره لاگ میکروتیک که ببنیم چه اتفاقاتی روی روتر رخ می دهد یا اینکه با راه اندازی پروکسی سرور ببنیم یوزرها در چه سایتی می روند.

اولین قدم راه اندازی لاگ سرور هست با یک سرچ درون گوگل می تونم بسیار لاگ سرور پیدا کنیم اگه عبارت SYSLOG

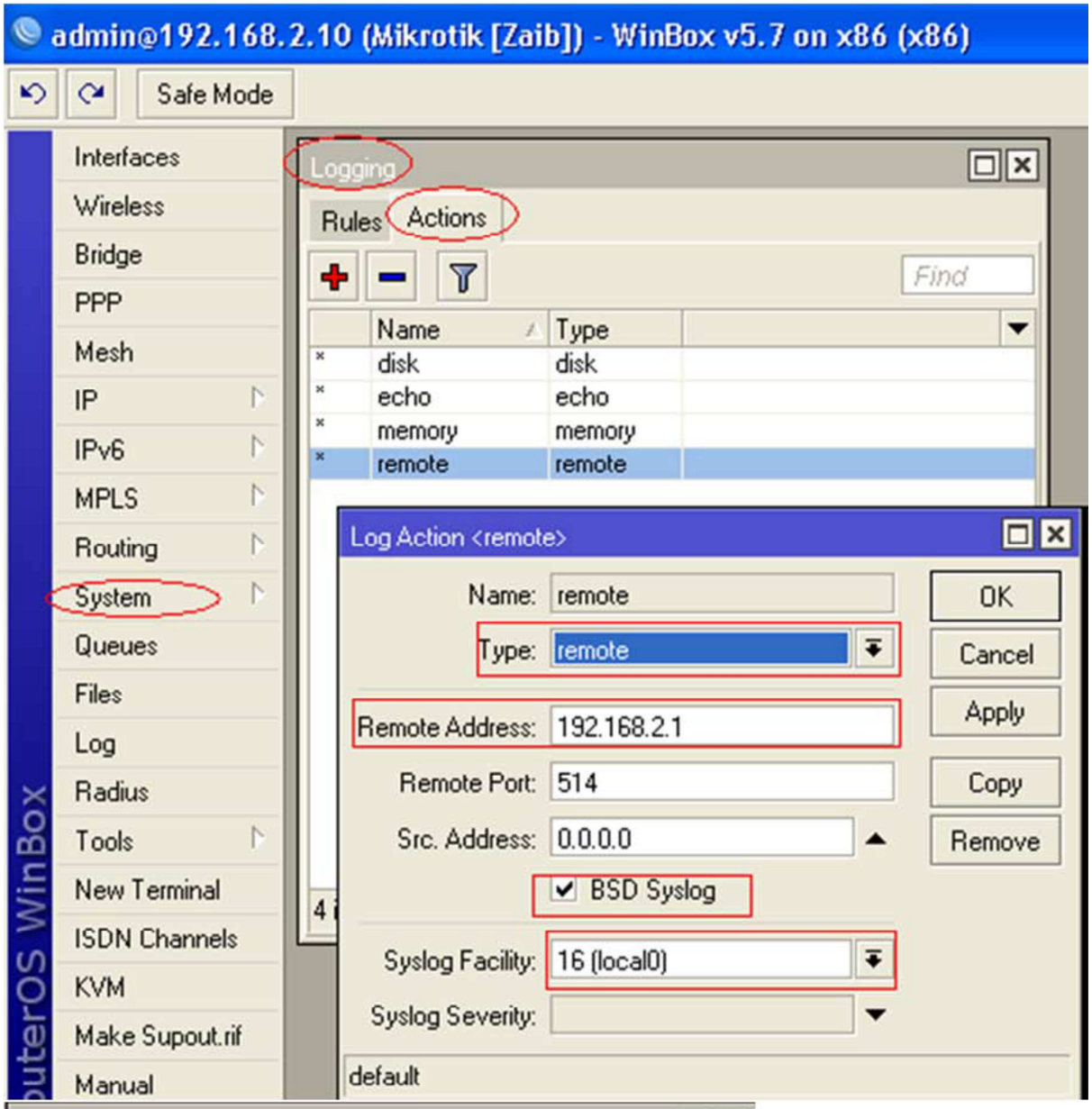
رو جستجو کنید برای سیستم عامل های مختلف هست

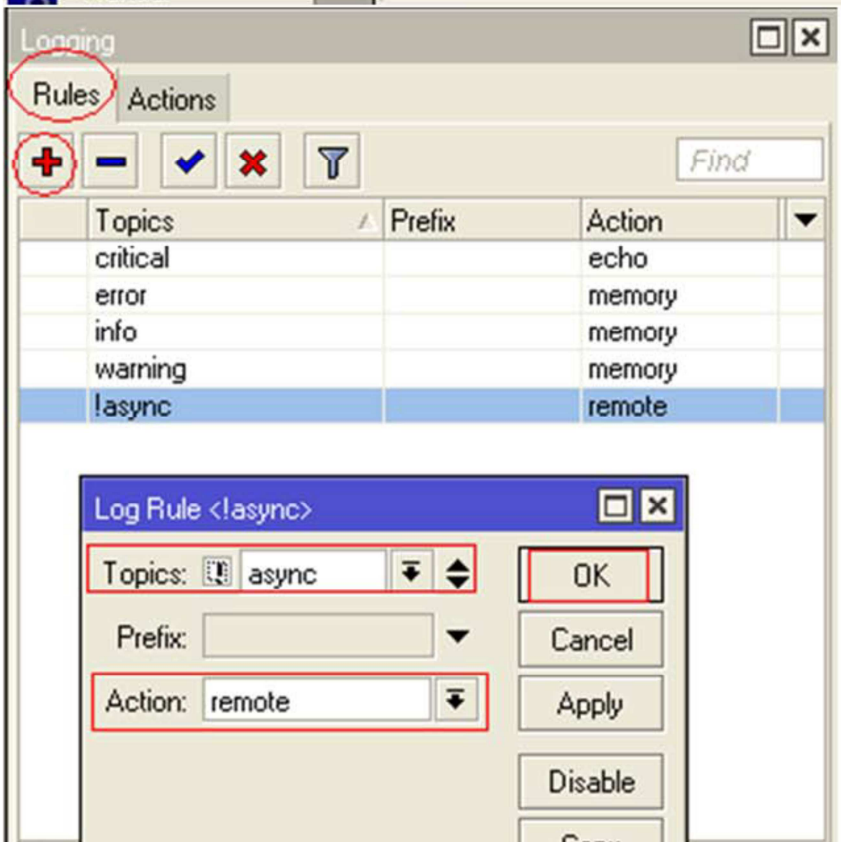
من پایه رو لینوکس می گذارم چون میکروتیک خودش قسمتی از لینوکس هست

قدم اول باید میکروتیک طوری تنظیم کنیم که logارو به یک سرور بیرونی انتقال بده نه روی Ramخودش

```
1 /system logging action
2
set remote bsd-syslog=yes name=remote remote=192.168.2.1 remote-port=514
src-address=0.0.0.0 syslog-facility=local0 syslog-severity=auto
target=remote
3 /system logging
4 add action=remote disabled=no prefix="" topics=!async
```

اینجا میگیم برو روی یک سرور بیرونی با آیپی ۱۹۲,۱۶۸,۱,۱


admin@192.168.2.10 (Mikrotik [Zaib]) - WinBox v5.7 on x86 (x86)
Safe Mode
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
Manual
RouterOS WinBox
Logging
Rules
Actions
Find
Name
Type
disk
disk
echo
echo
memory
memory
remote
remote
Log Action <remote>
Name: remote
Type: remote
Remote Address: 192.168.2.1
Remote Port: 514
Src. Address: 0.0.0.0
BSD Syslog
Syslog Facility: 16 (local0)
Syslog Severity:
default
OK
Cancel
Apply
Copy
Remove


Logging
Rules
Actions
Find
Topics
Prefix
Action
critical
echo
error
memory
info
memory
warning
memory
!async
remote
Log Rule <!async>
Topics: async
Prefix:
Action: remote
OK
Cancel
Apply
Disable

مرحله دوم می ریم سراغ لینوکس که لاگ سرور روش راه بندازیم

```
1 apt-get install syslogd
```

حالا نوبت دسترسی دادن به میکروتیک هست که بتوتی لاگش رو روی لینوکس ذخیره کنه

```
1 nano /etc/syslog.conf
```

```
1 !*
2 +192.168.2.10
3 local0.* /var/log/mt.log
```

۱۹۲,۱۶۸,۲,۱۰ میکروتیک من هست

```
1 touch /var/log/mt.log
2 chmod 600 /var/log/mt.log
```

با این کامند های بالا هم میکروتیک بتونه لاگش رو توی یک فایل جداگانه ذخیره کنه

سرویس لاگ رو ریاستارت می کنیم

```
1 /etc/init.d/sysklogd restart
```

و با این دستور درون کنسول لینوکس می تونیم لاگ رو ببنیم

```
1 tail -f /var/log/mt.log
```