

Разширен мониторинг в The Dude с функцията `ros_command`

София, MUM България 2019 г.

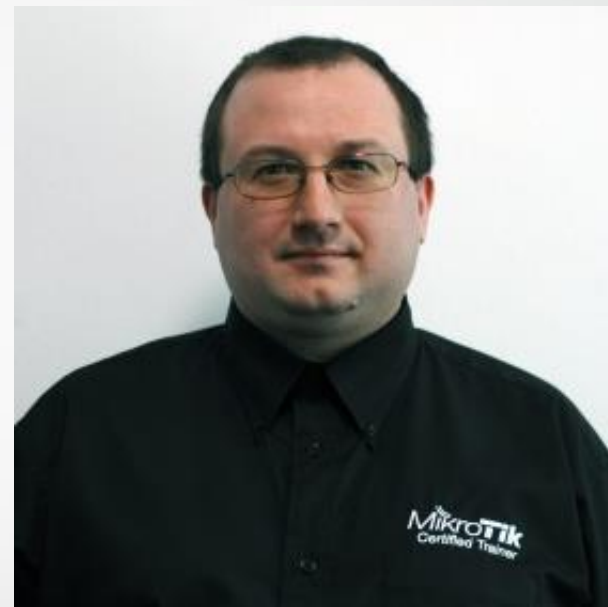
Петър Димитров

За мен:

ПГ НЕТ ПРО ЕООД

Компютърни мрежи:

- ❖ Персонализирани решения
- ❖ Обучения
- ❖ Консултантски услуги
- ❖ Проектиране, конфигуриране, мониторинг, диагностика и отстраняване на проблеми



Петър Димитров

Разширен мониторинг в The Dude, Петър Димитров

© PG.NET.PRO

The Dude

- ❖ Безплатен софтуер на MikroTik за наблюдение на мрежови (и други) устройства
- ❖ Автоматично откриване и добавяне към картата на устройства
- ❖ Наблюдение на услуги и уведомяване
- ❖ Поддържа наблюдение по SNMP, ICMP, DNS и TCP

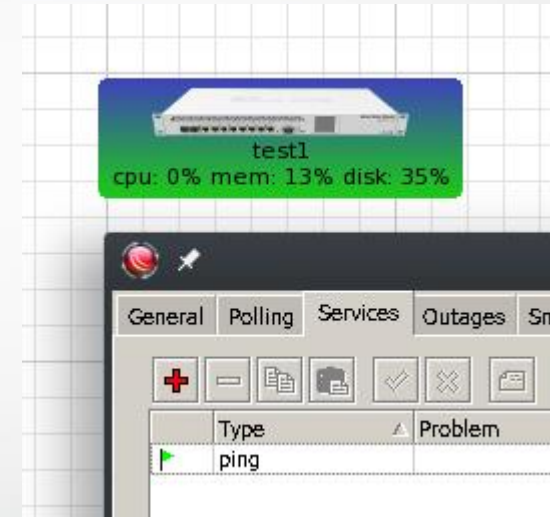
Защо The Dude, а не друг NMS?

- ❖ Възможност за централизиран достъп за конфигурация и управление на всички устройства (с winbox, terminal, ...)
- ❖ Възможност за масов контролиран upgrade/downgrade и проследяване на версиите
- ❖ Множество инструменти, стартирани от устройствата
- ❖ Изпълнение на команда в RouterOS, което ни дава неограничени възможности за мониторинг

Базово наблюдение - ping



- ❖ За базово наблюдение обикновено използваме ping
- ❖ Така единствено знаем дали устройството е живо и достъпно



Информация по SNMP

- ❖ Някои параметри са достъпни по SNMP
- ❖ Можете да проверите някои идентификатори в RouterOS с помощта на `print oid`:

```
[admin@home-core] > system health print oid
    active-fan: .1.3.6.1.4.1.14988.1.1.3.9.0
      voltage: .1.3.6.1.4.1.14988.1.1.3.8.0
      current: .1.3.6.1.4.1.14988.1.1.3.13.0
  temperature: .1.3.6.1.4.1.14988.1.1.3.10.0
cpu-temperature: .1.3.6.1.4.1.14988.1.1.3.11.0
power-consumption: .1.3.6.1.4.1.14988.1.1.3.12.0
    psu1-state: .1.3.6.1.4.1.14988.1.1.3.15.0
    psu2-state: .1.3.6.1.4.1.14988.1.1.3.16.0
[admin@home-core] >
```

Функции в The Dude

- ❖ За да използваме лесно информацията в The Dude, която можем да придобием по един или друг начин, можем да дефинираме функции
- ❖ Нека дефинираме функции за температури и статус на захранванията:

<code>snmp_mtk_temperature:</code>	<code>oid("1.3.6.1.4.1.14988.1.1.3.10.0")</code>
<code>snmp_mtk_cpu_temperature:</code>	<code>oid("1.3.6.1.4.1.14988.1.1.3.11.0")</code>
<code>snmp_mtk_psu1:</code>	<code>oid_raw("1.3.6.1.4.1.14988.1.1.3.15.0")</code>
<code>snmp_mtk_psu2:</code>	<code>oid_raw("1.3.6.1.4.1.14988.1.1.3.16.0")</code>

Функции в The Dude



The screenshot shows the 'New Function' dialog box in The Dude. The 'Functions' menu item in the left sidebar is highlighted with a red box. The dialog box contains the following fields:

- Name: snmp_mtk_temperature
- Description: Returns MikroTik temperature
- Code: oid("1.3.6.1.4.1.14988.1.1.3.10.0")

The background shows a table of existing functions:

Name	Error	Description	Notes
* and		logical and	
* array		returns array of given arguments	
* hdd_usage			
* if		first parameter - condition, second - returned if condition ...	
* link index		returns link index available from some contexts	

Разширен мониторинг в The Dude, Петър Димитров

© PG.NET.PRO

Визуализация в етикета

- ❖ Можем да визуализираме информацията в етикета на устройството, редактирайки го в Appearance:

```
[Device.Name]
[device_performance()]Temp/CPU:
[snmp_mtk_temperature()]C/[snmp_mtk_cpu_temperature()]C
PSU1/PSU2 State:[if((snmp_mtk_psu1())>0), "OK",
"FAIL"]/[if((snmp_mtk_psu2())>0), "OK", "FAIL"]
[Device.ServicesDown]
```

Визуализация в етикета



test1
cpu: 0% mem: 13% disk: 35%
Temp/CPU: 32.0C/55.0C
PSU1/PSU2 State:OK/OK

mcSettings
Appearance
Tools
Reprobe
Ack
Unack
Upgrade
Force Upgrade
Notes
Remove
Select Adjacent

[Device.Name] [device_performance()]Temp/CPU: [snmp_mtk_tem... "OK", "FAIL"]) [Device.ServicesDown] - Network Map Element

General Image

Type: item

Item Type: device

Map specific values of following settings are used for this item if not specified here

▼ Insert Variable Insert Oid Functions...

Label:
[Device.Name]
[device_performance()]Temp/CPU: [snmp_mtk_temperatura()]C/[snmp_mtk_cpu_temperatura()]C
PSU1/PSU2 State:[if((snmp_mtk_psu1())>0), "OK", "FAIL"]/[if((snmp_mtk_psu2())>0), "OK", "FAIL"]
[Device.ServicesDown]

Label Refresh Interval: default
default 1s 2s 5s 10s 15s 30s 1m 2m 5m 10m 15m 30m 1h 2h 3h 6h 12h 1d

Unknown: ▼
Up: ▼
Down Partial: ▼
Down Complete: ▼
Acked: ▼
Shape: ▼
Font: ▼

Ok
Cancel
Apply
Remove

Функция `ros_command`

- ❖ Връща резултата от изпълнението на подадени като параметър команда или скрипт в RouterOS на устройството
- ❖ Дава практически неограничени възможности The Dude да получава всякакъв вид информация
- ❖ Полезна за проследяване на нетривиални параметри на устройствата, като състояние на BGP връзки, OSPF съседни, VPN-и и други

Команда print в RouterOS

- ❖ Показва информация за наличните в определено меню обекти в различен формат
- ❖ С параметър count-only командата print връща само общия брой обекти
- ❖ Параметър where помага за филтриране на обектите по зададено условие:

```
[admin@home-core] > ppp active print count-only
```

```
18
```

```
[admin@home-core] > ppp active print count-only where service=ovpn
```

```
11
```

Мониторинг на BGP връзки

- ❖ За проследяване на BGP връзките ще са ни необходими:
 - ❖ Функция, получаваща информация за общия брой връзки
 - ❖ Функция, проверяваща броя установени връзки
 - ❖ Механизъм за не-проследяване на връзки при определени обстоятелства: няма да вземаме под внимание забранените връзки, както и тези със служебен коментар "donotmonitor"
- ❖ Ще изпълняваме с `ros_command` команда `print` с необходимите параметри

Мониторинг на BGP връзки



❖ ros_bgp_all:

```
ros_command("routing bgp peer print count-only  
where disabled=no and comment!=donotmonitor")
```

❖ ros_bgp_est:

```
ros_command("/routing bgp peer print count-only  
where disabled=no and comment!=donotmonitor  
and established")
```

Да редактираме етикета!



test1
cpu: 0% mem: 12% disk: 35%
Temp/CPU: 32.0C/55.0C
PSU1/PSU2 State:OK/OK
BGP peers total: 18
BGP peers established: 18

- Settings
- Appearance
- Tools
- Reprobe
- Ack
- Unack
- Upgrade
- Force Upgrade
- Notes
- Remove
- Select Adjacent

[Device.Name] [device_performance()]Temp/CPU: [snmp_mtk_tem... [ros_bgp_est()][Device.ServicesDown] - Network Map Element

General Image

Type: item

Item Type: device

Map specific values of following settings are used for this item if not specified here

▼ Insert Variable Insert Oid Functions...

Label:
[Device.Name]
[device_performance()]Temp/CPU: [snmp_mtk_temperature()]C/[snmp_mtk_cpu_temperature()]C
PSU1/PSU2 State: [if((snmp_mtk_psu1())>0), "OK", "FAIL"]/[if((snmp_mtk_psu2())>0), "OK", "FAIL"]
BGP peers total: [ros_bgp_all()]BGP peers established: [ros_bgp_est()][Device.ServicesDown]

Label Refresh Interval: default default
default 1s 2s 5s 10s 15s 30s 1m 2m 5m 10m 15m 30m 1h 2h 3h 6h 12h 1d

Unknown: ▼

Up: ▼

Down Partial: ▼

Down Complete: ▼

Acked: ▼

Shape: ▼

Font: ▼

Ok
Cancel
Apply
Remove

Разширен мониторинг в The Dude, Петър Димитров

Probes

- ❖ За проследяване във времето, за графики и най-вече за генериране на събития при настъпване на определени обстоятелства използваме Probes
- ❖ За проследяване състоянието на BGP връзките:
 - ❖ Дефинираме Probe от тип функция
 - ❖ Задаваме условие, проверяващо състоянието
 - ❖ Указваме при нормално състояние каква стойност се връща и в каква мерна единица

Дефиниране на Probe



The screenshot shows the 'New Probe' dialog box in The Dude. The 'Contents' pane on the left has 'Probes' highlighted. The dialog box has the following fields and content:

- Name:** bgp_all_up
- Type:** Function
- Agent:** default
- Description:** Performs custom functions to decide if service is available and up. If up graphs value of another function. Should return true if service is available.
- Available:** 1
- Notes:** If return string is empty then service is assumed up
- Error:** `if(ros_bgp_est()==ros_bgp_all(),"",concatenate(ros_bgp_all()-ros_est()," BGP peer(s) DOWN!"))`
- Value:** `ros_bgp_est()`
- Unit:** peers

Buttons on the right: Ok, Cancel, Apply, Notes, Copy, Remove.

Разширен мониторинг в The Dude, Петър Димитров

Добавяне на Probe към устройство



test1
cpu: 0% mem: 13% disk: 35%
Temp/CPU: 32.0C/55.0C
PSU1/PSU2 State:OK/OK
BGP peers total: 18
BGP peers established: 18


The screenshot shows the 'test1 - Device' window in The Dude. The 'General' tab is active, displaying a table with one row: 'ping' under the 'Type' column. Overlaid on this is the 'New Service' dialog box. The 'General' tab of the dialog is selected, showing the following configuration:

- Device: test1
- Probe: bgp_all_up
- Agent: default
- Enabled:
- Probe Port:
- Probe Interval: default (with a slider from default to 30s, 15m, 6h)
- Probe Timeout: default (with a slider from default to 30s, 15m, 6h)
- Probe Down Count: default (with a slider from default to 5, 8, 12, 20)
- Status: unknown
- Problem: (empty)
- Probes Down: 0
- Time Last Up: 00:00:00
- Time Last Down: 00:00:00
- Time Up: 00:00:00
- Time Down: 00:00:00

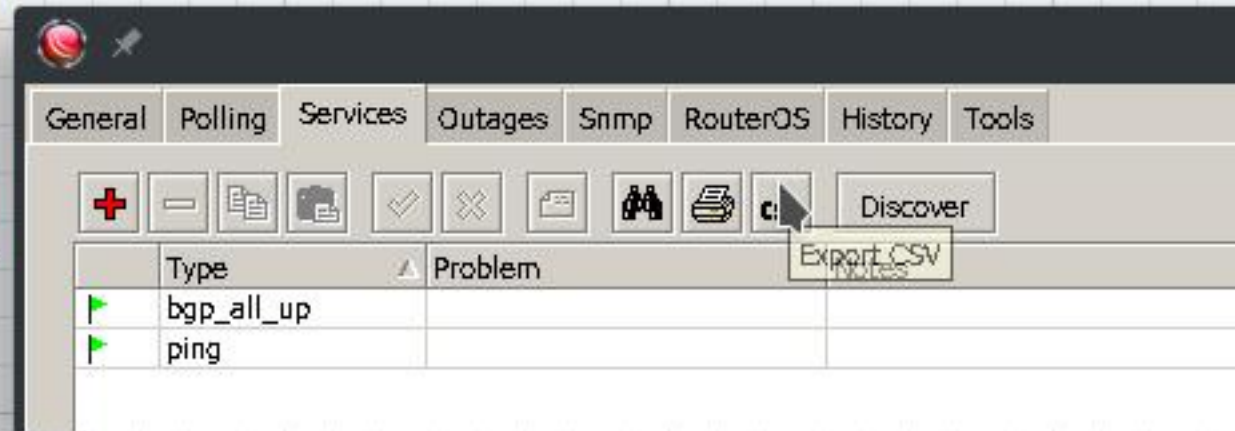
Buttons on the right side of the dialog include: Ok, Cancel, Apply, Notes, Copy, and Remove.

Разширен мониторинг в The Dude, Петър Димитров


Резултат:



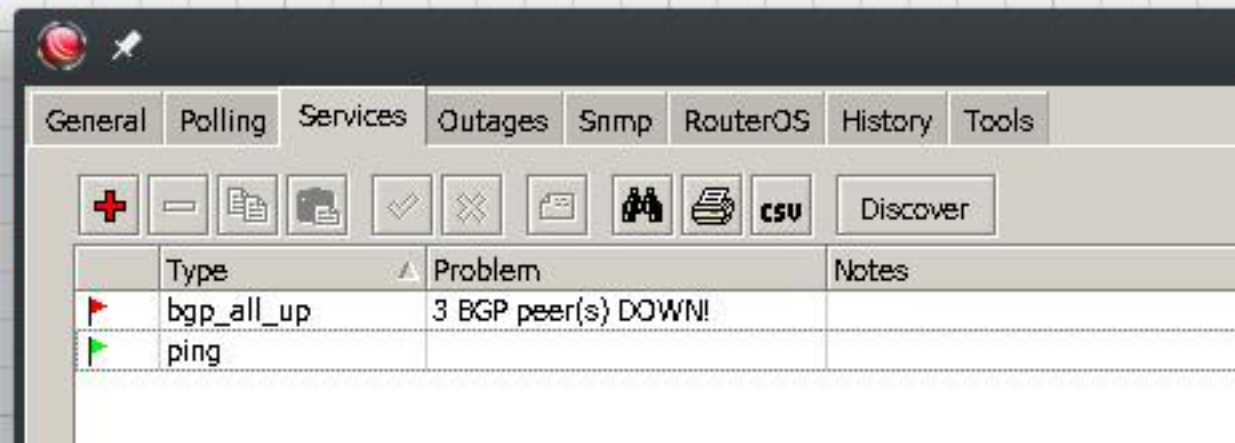
test1
cpu: 0% mem: 13% disk: 35%
Temp/CPU: 32.0C/55.0C
PSU1/PSU2 State:OK/OK
BGP peers total: 18
BGP peers established: 18



Type	Problem
bgp_all_up	
ping	



test1
cpu: 0% mem: 13% disk: 35%
Temp/CPU: 32.0C/55.0C
PSU1/PSU2 State:OK/OK
BGP peers total: 18
BGP peers established: 15
bgp_all_up



Type	Problem	Notes
bgp_all_up	3 BGP peer(s) DOWN!	
ping		

Разширен мониторинг в The Dude, Петър Димитров

Notifications

- ❖ За да получим информация за настъпило събитие (например отпадане или възстановяване на услуга) използваме Notifications
- ❖ За уведомяване по електронната поща:
 - ❖ Дефинираме Notification от тип email
 - ❖ Конфигурираме параметрите за работа със сървъра
 - ❖ Указваме съдържание за Subject и Body

Notifications

The screenshot displays the 'Notifications' configuration window in The Dude. The left sidebar shows the 'Notifications' menu item highlighted. The main window is titled 'New Notification' and contains the following fields:

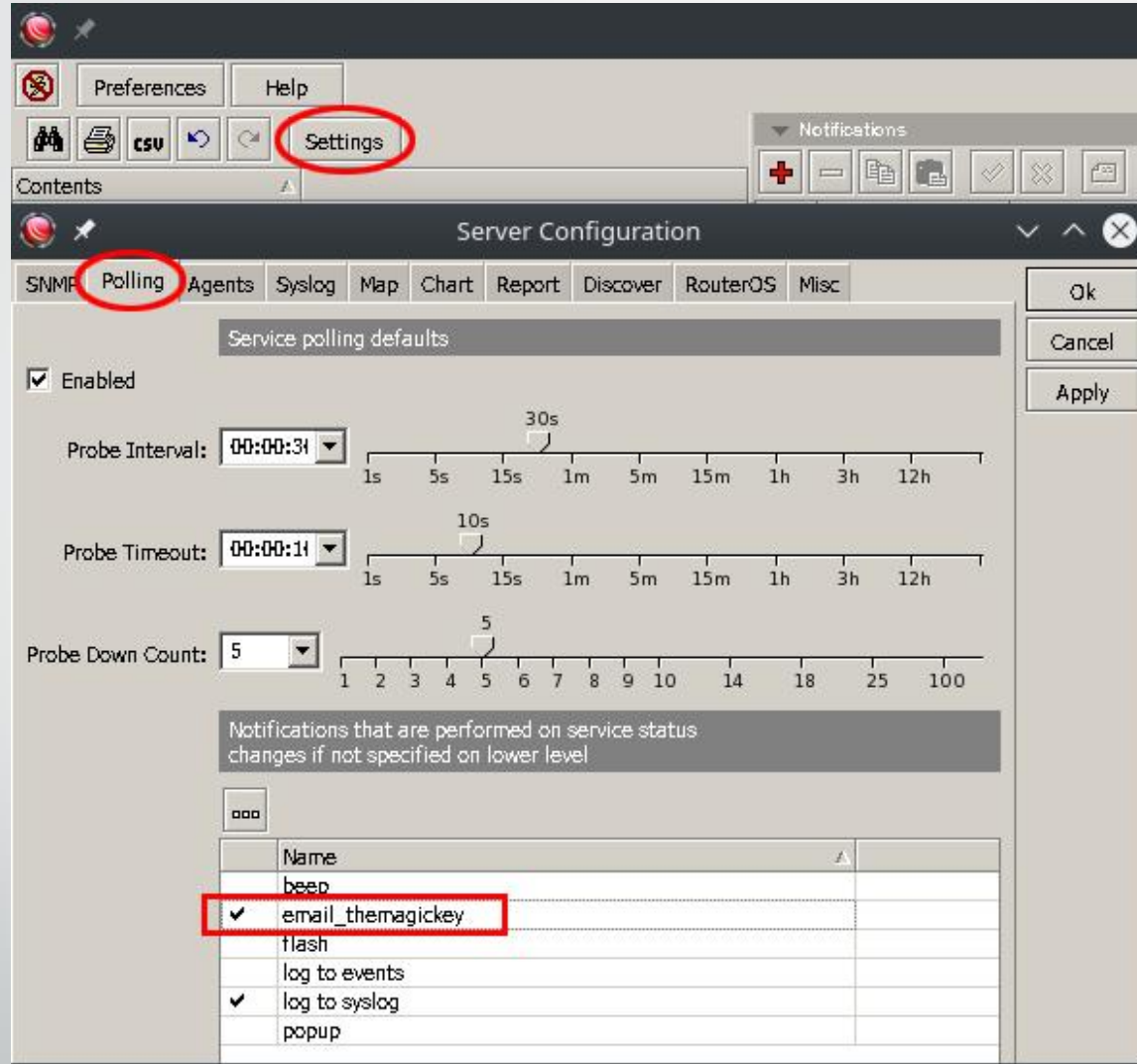
- Name:** email_themagickey
- Enabled**
- Type:** email
- Server IP:** (empty)
- Server Dns Name:** pgnetpro.bg
- Server Port:** 465
- User:** testdude@pgnetpro.bg
- Password:** [masked]
- Tls Mode:** tls-only
- From:** testdude@pgnetpro.bg
- To:** training@pgnetpro.bg
- Cc:** (empty)
- Subject:** Service [Probe.Name] on [Device.Name] is now [Service.Scatus]
- Body:** Service [Probe.Name] on [Device.Name] is now [Service.Scatus] ([Service.ProblemDescription])

Разширен мониторинг в The Dude, Петър Димитров

Notifications

- ❖ Активирането и използването на Notifications може да се управлява на различни нива:
 - ❖ Глобално за The Dude
 - ❖ По-специфично за определена карта
 - ❖ Най-специфично за конкретно устройство

Notifications



Разширен мониторинг в The Dude, Петър Димитров

Използване на get и put

- ❖ Команда get взема стойността на указания параметър за избрания обект
- ❖ Вложена команда find помага за филтриране на обектите по зададено условие
- ❖ За да върнем резултат, който ros_command да получи, използваме команда :put

```
:put [/ip address get value-name=address [find where interface=ether2]]
```


Използване на get и put

- ❖ За да визуализираме публичния си адрес, който сме получили динамично, ще направим:
 - ❖ Функция, получаваща адреса с `ros_command`
 - ❖ Ще редактираме отново етикета
- ❖ По този начин можем да получим всяка стойност на параметър в RouterOS
- ❖ Аналогично с `ros_command(":put $myvariable")` можем да получаване и стойности на глобални променливи от RouterOS, които се инициализират/актуализират в рутера

Резултат:



The screenshot displays two windows from The Dude network management software. The top window, titled "ros_public_ip - Function", is used to define a custom function. It has the following fields:

- Name: `ros_public_ip`
- Description: `Returns IP on ether2-inet`
- Code: `ros_command(" :put [/ip address get value-name=address [/ip address find where interface=ether2-inet])"`

The bottom window, titled "[Device.Name] [device_performance()]Public IP: [ros_public_ip()][Device.ServicesDown] - Network M...", shows the configuration for a device. It includes the following details:

- General tab selected
- Type: `item`
- Item Type: `device`
- Map specific values of following settings are used for this item if not specified here
- Buttons: `Insert Variable`, `Insert Oid`, `Functions...`
- Label: `[Device.Name] [device_performance()]Public IP: [ros_public_ip()][Device.ServicesDown]`
- default

On the left side of the interface, there are two device cards with their respective statistics:

- Device 1:** `172.22.22.254`
cpu: 0% mem: 51% disk: 86%
Public IP: 10.0.0.222/24
- Device 2:** `test1`
cpu: 0% mem: 12% disk: 35%
Temp/CPU: 32.0C/55.0C
PSU1/PSU2 State: OK/OK
BGP peers total: 18
BGP peers established: 18

Още няколко идеи...

```
ros_command("/ppp active print count-only")
```

```
ros_command("/routing ospf network print count-only where disabled=no")
```

```
ros_command("/routing ospf neighbor print count-only")
```

```
ros_command("/interface wireless registration-table print count-only")
```

```
ros_command("/caps-man remote-cap print count-only")
```

```
ros_command("/caps-man remote-cap print count-only where (identity ~ \"AP23\")")
```

```
ros_command("/caps-man registration-table print count-only")
```

```
ros_command("/caps-man registration-table print count-only where (interface ~ \"AP23\")")
```

За какво може да послужи:

Наблюдаването/сравняването на стойностите на

```
ros_command("/ip firewall connection print count-only  
where tcp-state=syn-sent")
```

и

```
ros_command("/ip firewall connection print count-only")
```

Благодаря за вниманието!

Можете да ме потърсите след
презентацията, ако имате въпроси.

Полезни връзки:

Тази презентация можете да намерите на:

https://www.pgnetpro.bg/images/Presentations/extended_monitoring_wTheDude_ros_command.pdf

Официалната документация за The Dude:

https://wiki.mikrotik.com/wiki/Manual:The_Dude

Mikrotik VPS за The Dude можете да наемете на:

<https://www.bgocloud.com/>