

PCAP

libpcap (winpcap). , :
•
• (data-source) NETAMS4
, , , Ethernet, NETAMS4. PCAP, . Linux BSD, libpcap, Windows - DLL winpcap
: ?
: PCAP. ? Remote agent, ., Windows .
! PCAP (jnetpcap) *BSD ! Remote PCAP Agent .
Java VM, jnetpcap, JPCapLocalDataSource . Remote PCAP Agent.
PCAP NETAMS4 "-> ", JPCapLocalDataSource, , :
• , - , "" .
• - pcap . "ip", , pcap-fliters(7).
• - , promiscuous mode, .. , "" . "true/false".

Добавить новый источник

Наименование:

Статус:

JPcapLocalDataSource

Остановлен

ID: 5

Версия: 1.1

Тип: JPcapLocal

Статус

Конфигурация

Пуск

Стоп

Удалить

Источник данных: 5

Ключ	Наименование	Значение
ds_name	Имя источника данных	JPcapLocalDataSource
iface	Имя интерфейса, на котором принимать пакеты	\Device\NPF_{E4381F6A-0A08-4707-BC5B-F76D70FA13E1} { [INET4:172.16.130.1] }
rule	Правило фильтрации пакетов на интерфейсе	ip
promisc	Включить режим захвата всех наблюдаемых пакетов	false

Применить

Обновить

Закрыть

Linux UNIX , , ifconfig, "eth0" "rlo". Windows, , PCAP , GUID-. , "Local Are Connection #1" "\Device\NPF_{E4381F6A-0A08-4707-BC5B-F76D70FA13E1} ". JPcapLocalDatasource , "" . - jserver/logs/netams4.log :

```
discovered local iface \Device\NPF_{E4381F6A-0A08-4707-BC5B-F76D70FA13E1}]
discovered local iface \Device\NPF_{896D57C9-4EBD-4B08-A667-6FD9633694E7}]
discovered local iface \Device\NPF_{78FE2F04-7C65-4EB2-AE78-7B03296C9294}]
```

, ipconfig.
, , "" .

: , Cisco, NetFlow (URL)?
: (IP-), , - (, VLAN) (SPAN-port, port mirroring) .