

MUHAMMAD REZAUL KARIM  
doing Network and system administration since 2005  
Trainee : bdnog 01 and bdnog 04  
Trainer: bdnog 08, 10/Sanog32  
and bdnog 11

= NETWORK MONITORING SYSTEM / NMS =

---

DISCLAIMER

## = LAB PREPARATION =

**LAB is behind VPN**

**Supporting Resource DOWNLOAD Link**

**<https://wfs1.redskybd.com/s/Wqds0f3A9QTq6en>**

**-Please Download The Resources**

**-Configure OpenVPN Client / SoftEther VPN Client in your Laptop  
(Instructors will help)**

**-Please Group Yourself / 3-personnel in each group**

Group # 00, remote lab Server # 00, IP # 172.16.108.70

Group # 01, remote lab Server # 01, IP # 172.16.108.71

Group # 02, remote lab Server # 02, IP # 172.16.108.72

Group # 03, remote lab Server # 03, IP # 172.16.108.73

Upto...

Group # 11, remote lab Server # 11, IP # 172.16.108.81

ssh-user id: bdnog11 / password: bdnog11cox / ssh-port: 1122

Please do “**sudo su**” after login to get root access.

## What is NMS:

---

Monitoring an active communications network in order to diagnose problems and gather statistics for administration and fine tuning. (PCMAG.COM)

The use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator in case of outages via email, pager or other alarms. It is a subset of the functions involved in network management. (WIKIPEDIA)

## Basic Workflow Functions:

---

- **DISCOVER**
- **DISPLAY**
- **MONITOR**
- **ANALYZE**
- **ALERT**
- **REPORT**
- **AUTOMATE**

## So Why USE NMS:

---

- Identifying unofficial services or servers.
- Monitoring usage and traffic statistics.
- Troubleshooting your network.
- Investigating a security incident.
- Keeping logs of users activities for accountability

## Types of Monitoring:

---

- a) Network Device Monitoring.
- b) Virtual & Physical Server Monitoring.
- c) Service/Application Monitoring.

## Some NMS application:

---

**NAGIOS, CACTI, SOLARWINDS, MRTG, PRTG, SYSLOG-NG, MUNIN, NTOP, ZABBIX, CHECK\_MK, OBSERVIUM, MONIT** etc.

## Simplest NMS Tools:

---

- PING
- TRACEROUTE

## **PING:**

---

- Measure the time for a packet to travel to a remote host and back.
- The server sends back an acknowledgment when the packet arrives.

## **TRACEROUTE:**

---

- List the router hops between the client host and a remote host.
- The IP address and domain name (if there is one) of each router is returned to the client.

## What is MRTG:

---

- Tool to monitor the traffic load on network links.
- MRTG generates HTML pages containing PNG images which provide a LIVE visual representation of this traffic.
- MRTG uses the Simple Network Management Protocol (SNMP) to send requests with two object identifiers (OIDs) to a device.

## Our Choice of NMS:

---

(01) CHECK\_MK/OMD & (02) OBSERVIUM

CHECK\_MK



## Agenda:

---

What is OMD?

What is Check\_MK?

Deployment (OMD and Check\_MK agent)



## What is OMD:

---

- Open Monitoring Distribution - <http://omdistro.org/>
- Not a Linux distro, just a group of tools

### Features:

- Multiple instances per host.
- Separate omd user per instance, etc.

## What is CHECK\_MK:

---

- Nagios add-on (Developed by Mathias Kettner)

### Features:

- Automatic Service-Detection
- Rule-based, hierarchical configuration
- High performance through passive checks
- Creates Nagios configs using web-UI.

## OBSERVIVUM



## Observium

---

- Auto-discovering SNMP based network monitoring tool
- Written in PHP (web application)
- Includes support for a wide range of network hardware and operating systems including:-Cisco, Linux, FreeBSD, Juniper, Brocade, Foundry, HP and many more.

-See

[https://www.observium.org/supported\\_devices/](https://www.observium.org/supported_devices/)

## Available Feature Metrics:

---

- CPU, Memory and Storage statistics.
  - Interface traffic, packet and detailed error statistics.
  - Temperature, Fan Speed, Voltage, Amperage, Power, Humidity and Frequency sensors.
  - Users, Processes, Load Average and Uptime statistics.
- 
- Linux distribution detection.
  - Real-time interface traffic graphing.
  - Device inventory collection (very useful!)
  - Detailed IPv4, IPv6, TCP and UDP stack statistics.
  - BGP and OSPF statistics.
  - MAC / IP

## What is SNMP?

### **SNMP # Simple Network Management Protocol**

- Industry standard, hundreds of tools exist to exploit it
- Present on any decent network equipment

### **Query # Response based: GET / SET**

- GET is mostly used for monitoring

**Runs on UDP protocol, port 161**

### **Different versions**

- V1 (1988) – RFC1155, RFC1156, RFC1157
  - Original specification
- v2 – RFC1901 ... RFC1908 + RFC2578
  - Extends v1, new data types, better retrieval methods
  - Used is version v2c (without security model)

**-v3 – RFC3411 ... RFC3418 (w/security)**

**Typically we use SNMPv2 (v2c)**

### **Typical queries**

- Bytes In/Out on an interface, errors**
- CPU load**
- Uptime**
- Temperature or other vendor specific OIDs**

### **For hosts (servers or workstations)**

- Disk space**
- Installed software**
- Running processes**
- ...**