Network Monitoring

What is Network Monitoring?

Network monitoring is the use of a system that constantly or periodically monitors a computer network for slow or failing components and that notifies the network administrator in case of outages or other trouble

Why use a Network Monitoring System?

- To optimize network performance and availability
- Stay informed
- Diagnose issues
- Report issues
- Eliminate the need for manual checks
- Proactive approach
- Track trends

How Network Monitoring Systems Works?

- Collect data from devices periodically
- Use different protocols
  - SNMP
  - ICMP
  - Netflow
- Set up a baseline
- Check if the data values with the base line
- Notify if values are below the baseline

Network Monitoring Tools

- Open Source
  - Cacti
  - LibreNMS
  - Nagios
  - Zabbix
- Commercial
  - GFI LanGuard
  - Microsoft Network Monitor
  - PRTG

What to Consider Selecting a NMS

- Deployment model
- Ease of use
- Compatibility with existing network infrastructure
- System scalability
- Interoperability

LibreNMS

Introduction

- SNMP-based auto-discover network monitoring
- Derived from Observium
- Written in PHP as a web application
- Includes support for a wide range of hardware

Technical Overview

- Linux distribution detection
- Real-time interface traffic graphing
- Device inventory collection (useful!)
- Detailed IPv4, IPv6, TCP and UDP stack statistics
- BGP And OSPF information
- Mac and IP address information
- Application monitoring using SNMP
- Integration with other tools

Features

- Dashboard
- Status Map
- Many Extensions, including:
  – Host monitoring well supported using check_mk and support scripts
  – Billing module
- Integration with other tools:
  – Smokeping, collectd, syslog (receive logs from devices)/graylog, Rancid/Oxisized (config management)

Philosophy

- LibreNMS' approach is that the network monitoring shouldn't take long to setup
  – You've already worked hard to build your network and configure it
  – LibreNMS is easier to understand if you understand it philosophy
- Configure equipment correctly
  – Community
  – xDP (CDP or LLDP)
  – SysName, sysLocation
- LibreNMS will do the rest
  – Auto discovery of devices and resources
  – Option use of sysServices to map which services (ports) are running on a device
- Concept of enabled vs. ignored
  – By default, LibreNMS will monitor (collect data) all ports/interfaces it finds.
  – If a port is configured to be up, but it's operationally up, LibreNMS will complain about
  – Tell LinreNMS to ignore these ports or better, shout them down if they're not used
  – When they're used, bring them up

Thank You