Network Monitoring

28th November 2017

IT Center,
University of
Peradeniya

Dilum Samarasinhe
(LEARN)

Overview

- Neywork Monitoring System
- Cacti
- LibreNMS

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

Cacti Network Monitoring System

Introduction

- A tool to monitor, store and present network and system/server statistics
- Designed around RRDTool with a special emphasis on the graphical interface
- Almost all of Cacti's functionality can be configured via the Web.

RRDtool

- Round Robin Database for time series data storage
- Command line based
- Made to be faster and more flexible
- Includes CGI and Graphing tools, plus APIs
- Solves the Historical Trends and Simple Interface problems well as storage issues

General Description

- Cacti is written as a group of PHP scripts.
- The key script is “poller.php”, which runs every 5 minutes
- Cacti uses RRDtool to create graphs for each device and data that is collected about that device. You can adjust all of this from within the Cacti web interface
- The RRD files are located in /var/lib/cacti/rra when cacti is installed from packages

Advantages

- You can measure Availability, Load, Errors and more all with history
- Graphics
- Data Sources
- Data Collection
- Templates
- Cacti Plugin Architecture
- User Management

Disadvantages

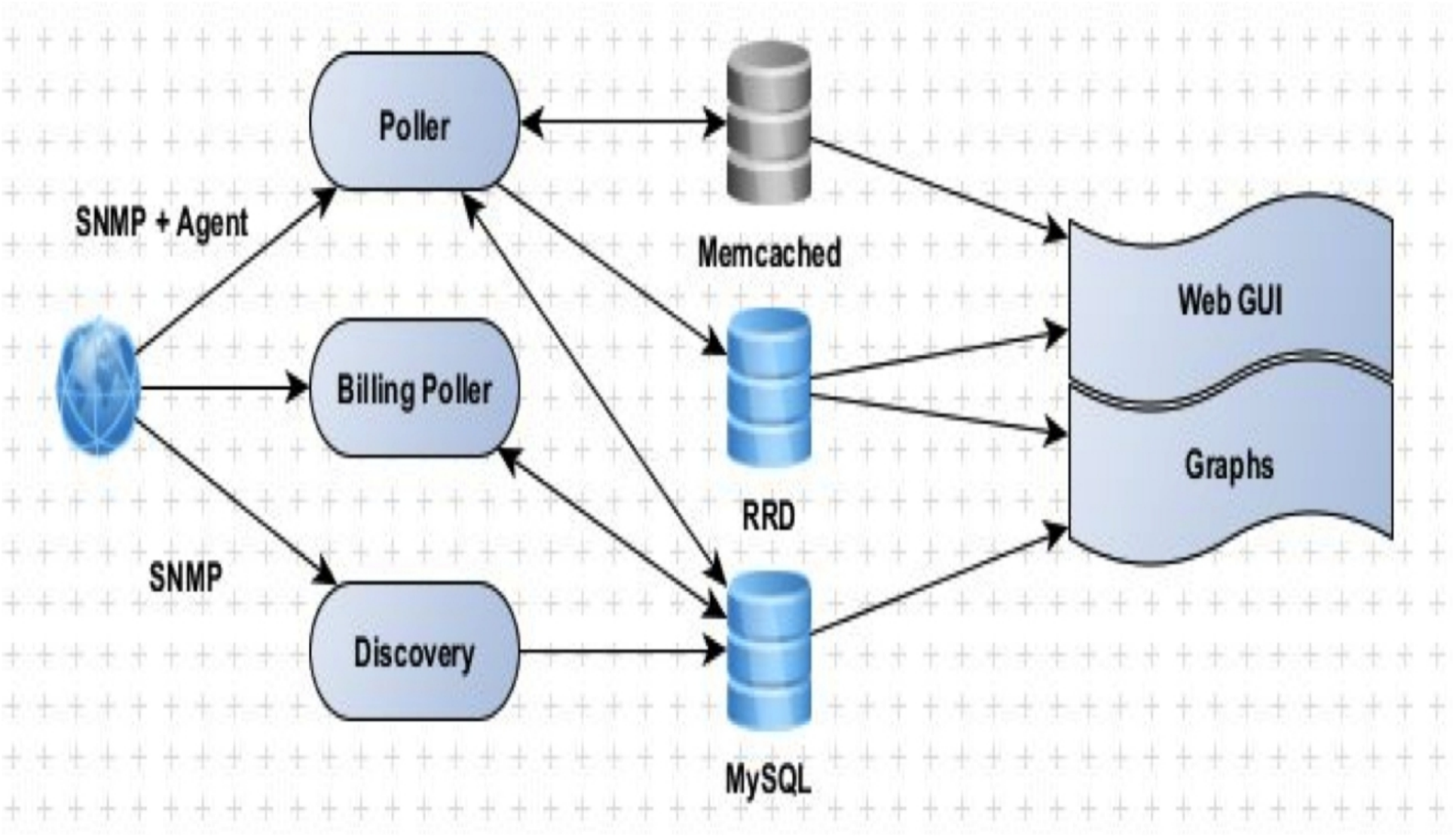
- Configuring Interfaces via the web interface is tedious
- Use provided command-line scripts instead
- Upgrading versions difficult if installed from source

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

Architecture



Features

- 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

Philosophy

- LibreNMS' approach is that the network monitoring shouldn't take long to set up
- Configure equipment correctly and LibreNMS will do the rest
- Concept of enabled vs. ignored
- Online LibreNMS demo Is available at:
  - https://demo.librenms.org/
  - Log on as demo / password : demo

Thank You

Dilum Samarasinghe/LEARN

Email: dilum@learn.ac.lk