MIECT: Integrated Management of Networks and Services 2011-12

1st Project: Distributed Monitoring

Deadline: Nov 17th v1.0

1 Objective

Acquire experience with distributed monitoring, performance monitoring and event tracking systems. Acquire practical experience with Round Robin Databases, SNMP and other remote monitoring technologies.

2 Description

The purpose of this project is to develop a distributed monitoring system, able to track system and service performance metrics, from the local host or several remote hosts. Taking in consideration the operating system of the remote host, and the metric, data can be gathered using SNMP, WMI, by directly probing the host, or any other technology found appropriate. For this assignment the support for SNMP is mandatory.

Each host should have one or more services defined, as well as information regarding the monitoring method, the interval between verifications, and the notification method. A scheduler should iterate over the definition of the hosts and verify service availability.

All data gathered should be stored in a Round Robin Database for later visualization with intervals of increasing size until an interval of 1 year between data points. The minimum interval considered should be of 5 minutes. Another form of database may be used to log events and display status information.

For each metric and system, thresholds may also be set so that a notification is sent to the system administrators and an alarm state is triggered for the service or host. The notification should be sent periodically until the issue is marked as acknowledged. Email support is mandatory for notification of

events, but others may be used.

Students should consider the following metrics, others may be considered:

- CPU: load percentage.
- Network Interface: used bandwidth, cumulative traffic, interface state (optionally with SNMP trap support).
- Service availability: TCP port open, response time.
- Storage: Used and available capacity.
- Memory: Memory used, free, cached and swap (if available in the system).
- Host: ICMP response time, End to End packet loss.

The following status should be considered:

- UNKNWOWN: No data is available regarding the system or server. All new systems and servers start with this status.
- OK: Threshold are no violated, and the system is considered to be functioning perfectly.
- WARNING: The first threshold was exceeded, but the second threshold was not exceeded.
- CRITICAL: The second threshold was exceeded.
- ERROR: It is impossible to verify the service or system.

The monitoring system should have a visualization interface allowing the display of the data stored in the RRD databases as well as the status (up/down/warning/critical) of each service and host. An appropriate way is to display a dashboard with summary status information, and then detailed information in different pages. Web technologies are suggested as the most appropriate way of showing this information, but others can be used.

Any programming language can be used to implement this project. Due to the tools and libraries available, interpreted languages such as PHP, Perl or Python may facilitate development.

3 References

- SNMP:http://www.net-snmp.org
- WMI Client for Linux: http://dev.zenoss.org/svn/trunk/inst/externallibs/wmi-1.3.13.tar.bz2
- RRDtool:http://oss.oetiker.ch/rrdtool