NETWORK PERFORMANCE MONITORING SYSTEM FOR LAKESHORE HOSPITAL, ATLANTA

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The aim of this project is to implement a network monitoring using an open source network management utility to check the state of network elements and associated services for Lakeshore hospital Atlanta. Such management tools must have capability to detect and respond to faults in the network by generating appropriate alert to notify the system administrator accordingly. Nagios enables data-driven insights and helps in decision making. Monitoring not only helps in preventing IT disasters, it also has a lot of other advantages. We can improve productivity and performance using this data. It prevents downtime and business losses. It can also help to cut down a company's budget and increase savings.

There are numerous open source and off-the-shelf network management applications that can be used to handle network monitoring & management issues while the selection can be based on the network requirement. In this project, an open source network management application named Nagios will be employed. This network management application is used to examine and demonstrate network monitoring of the network infrastructure and provision of alerts when modifications or problems are detected

Nagios core was used as the network management utility for the network for demonstration of monitoring exercise. Nagios was configured with its plug-ins and used against network run in the Linux environment. Furthermore, the implementations of Nagios for optimal performance can be laborious, but the experiences with Nagios and its resourceful outcomes proved to be worthwhile. Nagios is therefore recommended for use in companies and institutions for monitoring their networks.

. In general, network management functions include verification of the status of all network devices such as routers, switches, hubs and computers. NM also entails recording and analyzing error messages from all the aforementioned devices in order to monitor the health of all devices. Performance management is the top level network management operation. It is responsible for monitoring, controlling and optimizing the overall network performance, both within and across network services. Performance management includes functions such as gathering statistical information, maintaining and examining logs of the system state histories and altering system modes of operation for the purpose of conducting performance management activities.

INTRODUCTION AND PROJECT SCOPE:

Nagios is one of the most popular computer networks monitoring software application. It is an open source, Unix-based enterprise monitoring package with a web-based front-end or console. It provides monitoring of network services (SMTP, POP3, HTTP, FTP, SNMP, SSH) and host resources (processor load, disk usage, system logs) and essentially any device or service that have address and can be contacted via TCP/IP. It can monitor host running Microsoft Windows, Unix/Linux, Novell Netware, and other operating system.

Nagios is able to determine whether the hosts that are being monitored are in a DOWN or UNREACHABLE state. These are very different (although related) states and can help in quickly determining the root cause of network problems. Here's how the reach ability logic works to distinguish between these two states.

There are numerous open source and commercial products in the market for monitoring the network and the infrastructure. Some of the well-known open-source monitoring tools are Nagios, Zabbix, Cacti, Icinga, Groundwork, OpenNMS and Hyperic. Among these, Nagios is the most powerful tool. It is a framework that is capable of monitoring a large network of around 100,000 hosts and almost all components. Nagios can be integrated with third party tools. It uses the concept of modularity via plugins, which provide support for protocols, operating systems, system metrics, applications, services, Web servers, websites, middleware, etc.

Nagios does not have any internal monitoring logic. It is unaware of what is to be monitored and contains no built-in proprietary interpreters. It only does what it is instructed to do in a way one expects it to be done. Nagios lets the user intelligently schedule monitoring programs in any language. These monitoring programs are called plugins, which report the monitoring status back to Nagios. It has lots of hooks that make it easy to get data in and out; so it can provide real-time data to graphing programs such as RRDTool and MRTG, and can easily work along with other monitoring systems, either by feeding them or by being fed by them.

Example Network

Take a look at the simple network diagram below. For this example, let’s assume that all the hosts (server, routers, switches, etc.) that are pictured are being monitored. Nagios is installed and running on the Nagios host.

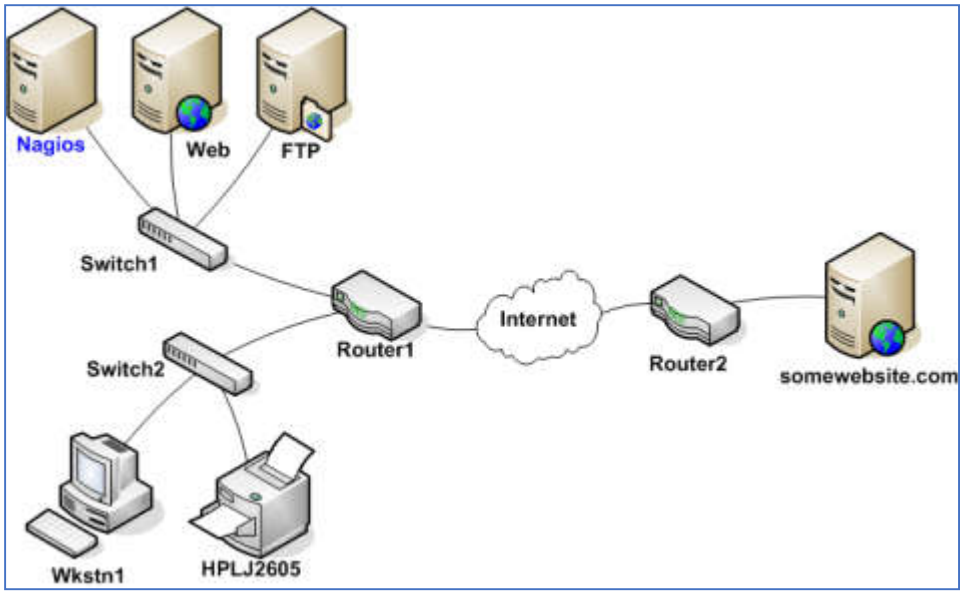


Figure 1: Simple Network Diagram

REASON FOR ISSUE/REISSUE:

When networks get busier it is very common, that the overall speed of these networks slows down. A lot of different trends are getting popular in the IT infrastructure like an increase in the use of cloud servers, video, VOIP etc. All these trends put tremendous pressure on IT infrastructure resources. When the stress on any network increases, it is very common for the companies to monitor network traffic with the help of network monitoring software. The best way to identify the kind of network traffic and its source is the Nagios.

Nagios XI is a really powerful system that offers quite a lot for infrastructure monitoring and creating reports on what is observed. The tool possesses a variety of configuration options, which are quite easy to use.

TERMS AND ABBREVIATIONS

SMTP:	Simple Mail Transfer Protocol
HTTP:	Hyper Text Transfer Protocol
SNP:	Snarl Network Protocol
POP3:	Post Office Protocol
PING:	Packet Internet Groper

PROJECT COST

Nagios XI has two distinct editions with three options each when it comes to pricing and licensing as mentioned below:

- **Standard Edition:** This edition costs $1,995 for 100 maximum nodes, $2,995 for 200 nodes, and $4,995 for unlimited nodes. Standard edition includes GUI configuration, reporting, visualizations, custom dashboards / views, notifications and more.
- **Enterprise Edition:** This edition costs $3,495 for 100 maximum nodes, $4,495 for 200 nodes, and $6,495 for unlimited nodes. Enterprise edition includes all the above listed features, as well as bulk tools, audit logging, SLA support, automated host decommissioning and more.

Please note that the Enterprise edition requires an annual renewal of the Maintenance and Support or Maintenance Only contract.

The renewal fees are listed below:

- Standard Renewal (Maintenance and Support): This option costs $1,650 for 100 nodes, $2,000 for 200 nodes, and $4,000 for unlimited nodes.
- Standard Renewal (Maintenance Only): This option costs $650 for 100 nodes, $750 for 200 nodes, and $1,500 for unlimited nodes.
- Enterprise Renewal Maintenance and Support): This option costs $2,400 for 100 nodes, $2,750 for 200 nodes, and $4,750 for unlimited nodes.
- Enterprise Renewal (Maintenance Only): This option costs $1,400 for 100 nodes, $1,500 for 200 nodes, and $2,250 for unlimited nodes.
- If the enterprise would like to add phone support, it can purchase either 5 calls for $995 or 10 calls for $1,495. These expire when the license expires.

REFERENCE DESIGN

This figure shows the design overview of Nagios monitoring server.

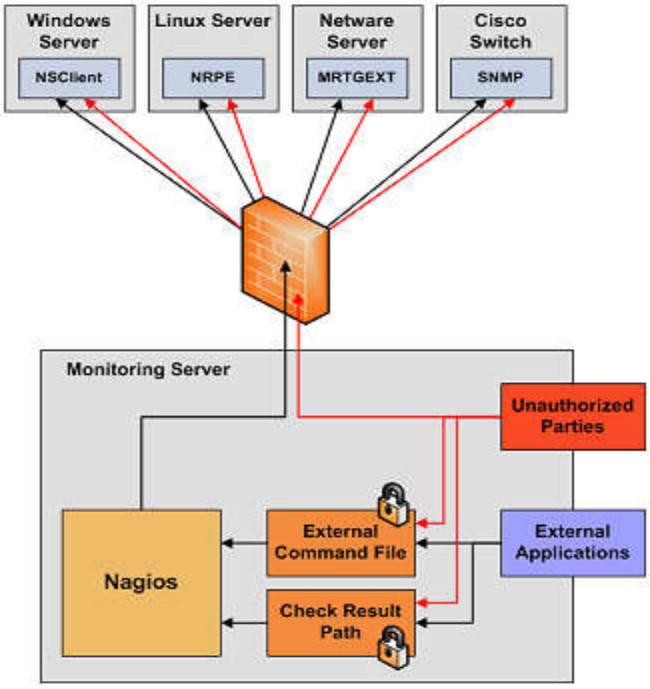


Figure 2: Design Overview of Nagios Monitoring Server

DATA CENTER DESIGN OVERVIEW

With the increasing need for computing power and space in data centers, server rack is often used to achieve high density. The server rack is a framework used for accommodating data center IT equipment such as servers, storage, HUB and network switches. It is designed to improve efficiency of data center network management and operation.

Network switches, router and Nagios server are placed in the server rack so the size of rack is look like this:

Figure 3: Racks

DESIGN REQUIREMENTS

- Network performance should be increased
- Alert problems immediately when required

HARDWARE REQUIREMENTS

- At least 20 GB of free hard drive space.
- 2 GB Memory or more.
- Dual Core 2.4 GHz CPU or faster.
- CentOS or RHEL (Red Hat Enterprise Linux) versions 5, 6, or 7.
- MySQL, plus PostgresQL if running versions less than Nagios XI 5 or upgrading from pre-5 version.

There are additional hardware requirements depending on monitored nodes / services.

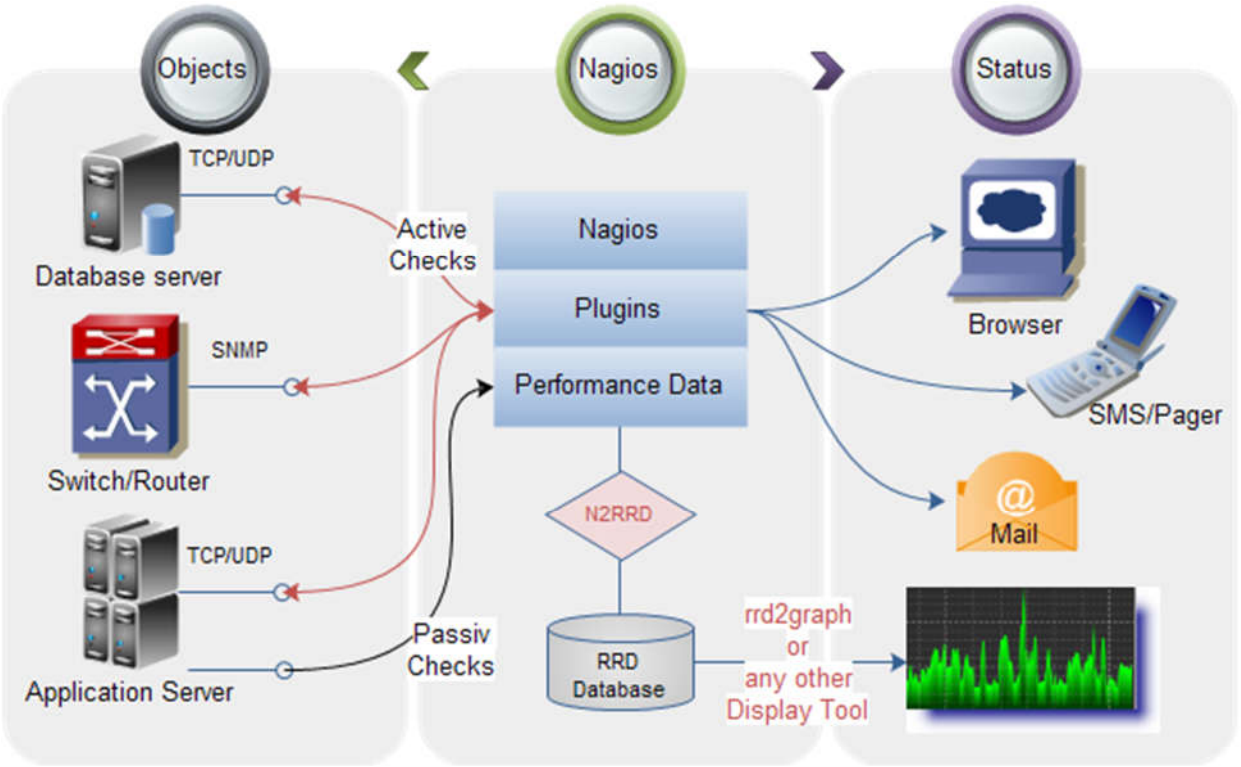
- 50 hosts, 250 services:
  At least 40 GB disk space, 1-2 cores, and 1-4 GB RAM.
- 100 hosts, 500 services:
  At least 80 GB disk space, 2-4 cores, and 4-8 GB RAM.

- More than 500 hosts, more than 2,500 services:
  At least 120 GB disk space, more than 4 cores, and more than 8 GB RAM.

If monitoring over 1000 hosts or 5000 services, a dedicated physical server is recommended.

DESIGN OVERVIEW

- Nagios is built on server/agents architecture.
- Usually, on a network, a Nagios server is running on a host, and Plugins interact with local and all the remote hosts that need to be monitored.
- These plugins will send information to the Scheduler, which displays that in a GUI.



CONFIGURING NAGIOS CORE

ENABLE SWITCH.CFG IN NAGIOS.CFG

Uncomment the switch.cfg line in /usr/local/nagios/etc/nagios.cfg

```
grep switch.cfg /usr/local/nagios/etc/nagios.cfg
cfg_file=/usr/local/nagios/etc/objects/switch.cfg
```

ADDING NEW HOSTGROUP FOR SWITCHES IN SWITCH.CFG:

The following switches hostgroup are added to the /usr/local/nagios/etc/objects/switch.cfg file.

```
define hostgroup{ hostgroup_name switches alias Network Switches}
```

New object definitions need to be created in order to monitor a new router/switch.

Open the **switch.cfg** file for editing.

```
vi /usr/local/nagios/etc/objects/switch.cfg
```

A new host definition is added for the switch that is required to monitor. If this is the *first* switch that is being monitored, the sample host definition in switch.cfg can simply be modified. The *host_name*, *alias*, and *address* fields are change to appropriate values for the switch.

```
define host {
   use         generic-switch          ; Inherit default values from a
                                                template
   host_name   abc                          ; the name we're giving to this
                                                switch
   alias       abc Switch               ; A longer name associated with
                                                the switch
   address     172.16.x.x               ; IP address of the switch


   hostgroups allhosts, switches        ; Host groups this switch is
                                                associated with
}
```

If the switch or router supports SNMP then lot of information can be monitored by using the *check_snmp* plugin.

The following service definition is added to monitor the uptime of the switch.

```
    define service {
   use                generic-service ; Inherit values from a template
   host_name          abc
   service_description Uptime
```

```
    check_command       check_snmp!-C public -o sysUpTime.0
}
```

CONCLUSION

Network monitoring is widely employed for the purpose of observing and analyzing the status and behaviors of the network and providing notifications to a network administrator through a messaging system, usually, emails, when a device fails.

Nagios provide us with an essential insight in our Network performance and availability. It has enabled us to respond quickly to errors in our network, and most importantly: it enables us to solve problems even before anyone notices the problems. In conclusion, in order to maintain and periodically verify the health status of network devices and associated services, the network performance should be monitored on regular basis. However, it is therefore clear that if organizations implement a network performance monitoring system, the outcome will essentially improve the network uptime and reduce the cost and save time of running the faults troubleshooting.

REFERENCES

1. https://www.thegeekstuff.com/2008/11/how-to-monitor-network-switch-and-ports-using-nagios/
2. https://opensourceforu.com/2018/07/nagios-a-modular-monitoring-tool-for-infrastructure-and-networks/
3. https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/networkreachability.html
4. https://www.motadata.com/blog/netflow-traffic-monitoring/
5. https://www.edureka.co/blog/nagios-tutorial/
6. https://www.howtoforge.com/tutorial/ubuntu-nagios/
7. https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/security.html