An Assessment of Document Clustering Based on KNMF Algorithm Applying Hadoop.

Bishnu Prasad Gautam and Dipesh Shrestha

● **Abstract**

There are lots of ways to monitor and manage the network. However, until date there are still large numbers of organization who are practicing network management without co-coordinating the tools and components into their system and time taken and the cost produced by these kinds of un-integrated practice is remarkable. To solve this problem, the integrated network management function is required to examine each subsystem regularly, and inform network administrator of error occurrence. In this paper we discuss how Nagios enables your network management capacity through monitoring functionalities and notification utility. Further we highlights the most important feature of Nagios and its capacity of alert and notification to the technical staff of the problem, allowing them to begin remediation processes before affecting the business processes, end-users, or customers of any organization. Our case study attempted of detecting and monitoring faults in a medium size network environment. The Nagios fault detection system is evaluated and its potentiality for self-healing and notification capabilities researched. This paper outlines possibilities of interconnecting Nagios with other applications in order to further facilitate and automate recovery after service failures thereby reducing the possible loss to the corporation. This case study also examines the role of network management in corporate management through utilization of monitoring tool named as Nagios.

● **Key words**

Network Monitoring, Notification, Capacity Planning

Introduction

Corporate of today without computer networks is hard to imagine as they have large numbers of computers in their office. These nodes are without doubt enabled with valuable resources and information. However, efficiency only can be achieved once these information nodes can share resources and support when they are placed in a Network. Companies with a supportive and reliable Network get an edge over the competitors. Network management is very essential part of corporate or any kind of organizational administration and maintenance of their networks. It involves not only the monitoring of health of the network but also proper management functions such as security, monitoring, control, allocation, deployment, coordination and planning. Network is monitored through large number of protocols and tools that exist for its support, including SNMP, CMIP, WBEM, Common Information Model, Java Management Extensions, NTOP, Netconf, MRTG and many others.

Considering the value Network provides to the organization, it is essential that it should equally receive proper management to advert losses due to problems in Network. Since Network links different heterogeneous components, chances are that at some point there arises a glitch in its operation. Aside from the human errors or computer failures, owing to its primal role in an organization, it can be a target for the attacks from the cyber criminal and unethical competitors as well. As organization grow the efficiency and reliability of its Network is increasingly becoming more important to the overall efficiency of the organization. Thus, a proper capacity planning, management and monitoring of network is required for organizational efficiency.

The Value of Network Monitoring in Corporate Management

"Network monitoring is like a visit to a cardiologist. You’re combining experience, judgment and technology to chart a system’s performance. Your doctor is watching for danger signs as blood flows through vessels, valves and chambers of the heart, while your network monitoring systems are tracking data moving along cables and through servers, switches, connections and routers" ,Network Monitoring Definition and Solutions, K. S. Nash, A. Behr [102]

Further, the other factor for practicing proper network monitoring is to deliver reliable computing power in order to maintain performance of the clusters or the networks into less physical space. It is quite certain that the increased density of nodes in networks can generate a significant amount of additional heat that often is not accompanied by increased cooling capacity. In our campus networks, we experienced a overheat problem which reacted to higher operating temperatures by increasing fan speeds. Once the temperatures get hot enough, we have to either limit CPU performance to reduce power consumption or increase cooling capacity of the room. In the case of running parallel applications, this reduction of CPU performance of one system may slow the performance of the entire networks which would not be the choice of Network administrator. However by using proper monitoring system, administrators can detect and address problems before they affect application performance.

Investing in the capacity planning, monitoring and management of network is a long term investment whose benefits although may not be precisely measured in money value (some work to measure benefits of security

investment has been done in [105], [106]), but can be expressed in terms of the orderliness, availability and risk minimization of information resources.

Network monitoring and management tools have evolved from simple commands like ping, traceroute etc to user-friendly and feature-enriched tools like Nagios, Ntop, MRTG as some of the open-source solutions and WhatsUp Gold , Total Network Monitor, CommView as commercial solution to name a few. Brief introduction of the Simple network commands and their usage by A.C. Davenhall & M.J. Leese can be found in [101] and a documented survey on network traffic monitoring and analysis tools can be found in [103].

In general a Network monitoring tools help to gain insight on the health of the network in following way

- the scheduled monitoring can detects failed condition
- create reports on the operational states of services.
- helps to analyze the resource utilization,
- understand the activities at each network nodes and identify potential failures

For our case study we chose Nagios owing to its architectural flexibility for configuration and advanced features like

- analysis of the patterns of operational states of hosts and services for capacity planning
- configurable problem notification system
- problem resolution options such as event handlers
- measurement of the additional overhead caused by its functioning
- remote monitoring

The Value of Capacity Planning in Corporate Management

Capacity planning in terms of computer networks is a process of determining the available resource in the networks in order to meet the demand of bandwidth, throughput and other hardware resources to the network users in a specified period of time. The key terms for capacity planning are identification of capacity and the effective management of the resources. An Inconsistency between the capacity of a network and the demands of the users might occur when a proper identification of available resources is not carried out. Equally, the need of identifying the components that negatively impact response time should not be overlooked. The goal of capacity planning is to minimize this inconsistency and avail the reliable network for its users. Demand for an organization’s capacity varies due to the changes in network resources, such as increasing or decreasing of the actual throughput of the networks and also the storage capacity. Capacity can be increased through introducing new techniques of management, adding extra machines, equipments and materials, increasing the number of network trouble shooters, and adding additional storage and bandwidth.

Corporate management can be obtained through executing a set of processes that help organizations optimize their business performance. The processes that affect the business performance must be monitored and this is not possible without the usage of network applications. These applications provide a framework for organizing business methodologies, metrics, processes and systems that drive business processes and the performance of the corporation.

Case Study Of Network Monitoring Through Nagios: A Summary of Nagios Functionalities and our Experiences

With a primary examination in our experimented scenario as well as sizeable secondary lab networks at WAKHOK we deployed Nagios that monitor at both locations to monitor more than 10-15 hosts at University lab and at our home-based network. With Nagios, we were fully able to monitor all of the nodes connected in network which is now able to run real time performance reports across their IT infrastructure as well as benchmark key performance metrics between the nodes. Having this facility allows for administrators of both systems to better collaborate to tune and tweak performance of their existing setup. We now can have centralized visibility into what's going on with our servers. We've really leveraged the open source architecture to accomplish very valuable customizations in regards to automatic alerts and alarms to help us mobilize quicker.

Nagios is an ideal tool for Capacity Planning of Network. Capactiy Planning with regards to Network relates to identification of the resources and services available in Network in one hand and the number of users that consume the resources and services in other hand. Balancing the serivce demand and supply is Capacity Planning in Network. Storage capacity (Hard disk spaces), transmission capacity (bandwidth), Processing Capacity(CPU state), Computation Capacity (Read/Write Memory) are some of the things that are to be considered under Network Capacity. With Nagios there are plugins to measure and continuously measure each of these physical resources. There are features to send notifications under the cirumtances that poses risk to proper functioning of Network. For instance there is a plugin named check_local_disk that measures the disk space of root partition and sends notification if the disk space is below some percentage of the total disk space. As an Network Administrator or Manager this vital information about the disk space helps to plan for the extension of new disk space or removal of unwanted files from the concerned disk. Obtaining such critical information before hand and preventing the disk from runnning out of space is proactive planning measure in Network. Similarly there are plugins to check the number of users or consumer, check_local_users which help to set a threshold level for maximum number of users accessing the system before a notification is sent to the concerned person. Understanding the number of time the notification is received and the period of day the notification is received a Network Manager can plan for the upgrade the capacity of that particular server as it is seen being accessed a lot.

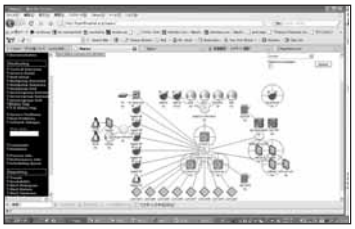
Bandwidth defines the flow capacity of the packets in the network. Just as the roads should match the number of vechical that run over it, the packets volume should be optimal to the bandwidth of network. With Nagios it's also possible to measure the bandwith over the routers or switches provided that MRTG program is installed. This plugin also helps to identify the bottlenecks in network and notify Network Managers promptly. Just like other capacity measuring plugins, with this plugin the actual utilization capacity of bandwith is provided and estimate the future trend of utilization.

Monitoring Campus Network with Nagios

The open source tool Nagios is a widely practiced network and system monitoring application. It provides a

Web based front end to display real-time services running in a host connected in a network for both stand alone host and group of cluster in a network. Nagios constantly checks the status of hosts and the services running in the host. There are number of plug-ins to check the status of the machines.

In our case studies, we have selected campus network having more than 10-15 hosts for monitoring purpose. We have installed Nagios in Ubuntu Machine and the Nagios was configured to monitor the hosts and the services. We have tested only the plain hosts that includeded, windows and linux machines. By default, Nagios monitors a collection of metrics, including http, current load, current users, Ping, root partition, Swap usage and total processes. It also provides a tool called status map that enables administrators to monitor the connected hosts in the network and shows the the set of visual graph it monitored. In this article we discusses Nagios version 3.0, which has lots of new features added in version 2.



Graphical representation of campus networks configured with nagios

Web Server Configuration

In order to run Nagios properly, we need to configure web server properly. The administrator in Nagios is given to nagioadmin user and we need to set the password during package installation. We need to configure the /etc/apache2/apache.conf file and enter the following directives into the file:

```
ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin

<Directory "/usr/local/nagios/sbin">
Options ExecCGI
AllowOverride None
Order allow,deny
Allow from all
AuthType Basic
AllowOverride None
Order allow,deny
Allow from all
AuthType Basic

ServerName localhost
AuthUserFile /usr/local/nagios/etc/htpasswd.users
Require valid-user
</Directory>

Alias /nagios /usr/local/nagios/share

<Directory "/usr/local/nagios/share">
Options None
AuthUserFile /usr/local/nagios/etc/htpasswd.users
Require valid-user
</Directory>
```

The directives of allow from all above, provides the accessibility from all IP. However, we can control the accessibilities with the following definitions:

Order Deny, Allow

Deny From All

Allow From 192.168.0.0/16

This will allow accessing Nagios only the IP starting from 192.168 and all other IP that does not match will be rejected.

Error and Recovery Alert

In order to properly manage the network, it is essential to view the overall status of the network at any time. However, it is equally important to get the notification while there is trouble in the network. Fortunately Nagios is supported with notification utility which sends the network administrator regarding the status of services and the hosts whether the services are running fine or not. Furthermore, we can use the package of existing check programs provided by Nagios or even add more check programs developed by ourselves or provided by other developers. It is also possible to setup time frames for the monitoring process as well as notifications when alarms arise. However, setting and configuring notifications is a tedious task in the beginning. We have used a send_gmail plugin[107] for notification which uses a pre-existing gmail user account to login into gmail SMTP server. Please refer the appendix for the details on installing the plugin.

Configuration of notification is carried out in contact.cfg file at which each contact is configured. We can also configure to whom the message should be sent and what would be the information in the message.

However, one should set a policy that in what situation the notification is sent. There are few situations that we consider to send the notifications such as:

-If the host or service is down or unreachable.

-If the host or service are not reliable and flapping.

-When the state of host or service is changed to Warning, Critical, Unknown or Ok

The notification is sent out after finding the current time period matches with the notification_timeperiod field from the host or service. It then extracts the list of contacts from contact_group fields and then checks whether each user's time period is included in the current date and time field. Once these kinds of criteria are met, Nagios will send a notification to each user. We have attached the notification message below sent by Nagios after the recovery of SSH service.

However, it is suggested from our case studies that we should select to whom the notification is sent. We can not send the notifications to each and every one who uses our network because sending too much information will create the panic and sometimes may loose the important information. Also it is not important to monitor each and every host and service in the network. We should monitor the most significant one rather than monitoring each service that has no significance in the network.

Host Management

Nagios also offers the web interface to change the configuration of hosts and its information. It offers the

view of all hosts, their status and the service running under each host. Network administrator sometimes loses remarkable amount of time to find which service is running under which host. This problem is more severe while the host is down and it is quite difficult to figure out the service running on specific host. However, this problem can be sorted out after the successful installation of Nagios at which one can define the service and keep the audit of each service in corresponding host. The following snapshot was the list of services running under my localhost at home. There is single host however once we configure the number of host with Nagios it will show the list of host under host menu.

Service Status Details for Hosts

Service Management

As like as host, Nagios has panels for managing and working with services running under corresponding host. Nagios manages service having each service and service group views. It also provides the web enabled interface to modify the parameters of the service. From this interface, network administrator can click in it and views the status of each service. It also provides detailed information of service, its status and other needful information.

Performance Information and other reporting

Nagios also provides the performance information page about the performance and the load of Nagios which can be accessed from the process info link. It describes the number of checks performed in a host and service and also gives the number of reports obtained from the external application.

The other feature that we found of the great importance during our case studies is its capability to prepare the reports. Any decision makers in the organizations can views the report regarding the management decisions. We can generate the reports on the basis of the object-type such as service, host, hostgroup, service group or any specified object. There are also the options for time period of report so that we can include the specific time period to generate the reports.

Conclusion

In order to manage the whole network of organization or corporation from a single system necessitates a tool having centrally monitoring support. It is very tedious to monitor each server in a standalone fashion. Nagios provides the centrally managed graphical tool for monitoring the networks thereby enabling the entire overview of network and its health. Without a tool having such capacity, it is very difficult to find out the network problem before occurring tremendous damage to its client, customer or users. Based in our University networks, we have set-up Nagios providing accurate and validated web analytics statistics for number of hosts containing huge size of data storage and services. With Nagios superior tracking technologies the tool is now able tracking all nodes which are configured and have capacity to fully monitor the intra-campus network having thousands of pages views a month. We conclude that Nagios can be used as the primary monitoring, capacity planning and

network management tool for any organization as their valuable IT infrastructure monitoring solution. Despite some success with Nagios, the IT management team should be updated with their capacity planning, unique needs, management and performance guarantees would require a more robust and scalable enterprise solution.

● References

[101] A.C. Davenhall & M.J. Leese,December 2005, An Introduction to Computer Network Monitoring and Performance, pp32-37

[102] K. S. Nash ,A. Behr, Network Monitoring Definition and Solutions, http://www.cio.com/article/133700/Network_Monitoring_Definition_and_Solutions?page=2#whyis

[103] Chakchai So-In, A Survey of Network Traffic Monitoring and Analysis Tools

[104] ESnet Network Monitoring Task Force (NMTF), "Network Monitoring Tools". http://www.slac.stanford.edu/xorg/nmtf/, http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html

[105] M. Cremonini, P. Martini, Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA),

[106] L. A.Gordon, M. P. Loeb, 2002, The economics of information security investment. ACM Transactions on Information and System Security 5, 4 (2002), 438-457.

[107] Open Solutions 101 http://www.opensolutions101.com/tips-tricks-information/nagios-smtp-gmail-notification/