Analyzer with Network Forensics and Notification

Shivakumar.K[1] Malarvizhi[2]
[2]Guide
[1,2]The Oxford College of Engineering

Abstract— As the corporate world grows the business also grows across the world, big business houses have the offices all over the world and even all clubbed so network management is very complicated and critical but with our application all the network analysis functionality can be managed at one place. It can be used for problem solving, collecting data flows, mapping, monitoring, collecting data, network forensics etc. Network related probes are very important for network management it supports multiple locations, departments, functions and users. Its single console gives the power to the admins to manage, monitor, and troubleshoot from any location. It helps to manage critical corporate infrastructure. Application helps in network monitoring and overview packet movements and about source & destination. User can identify traffic issues and diagnoses network slowdowns. Application is very simple to use and gives real time statics about the activities. Application converts all the related statics in charts also so that monitoring is easier. In conclusion, the application can collect and display statistics from several networked computers, as well as to control incoming and outgoing traffic in real time, so it’s important for network administrator. Multiple sensors and remote probes are supported by the application to monitor multiple segments from centralized console;

Key words: Probe manager, Maps, Notifications

I. Introduction

The actual monitoring is performed by Application probe processes which run on one or more computers. During installation the so-called Local Probe is automatically created by the system. In a single-probe installation—which is the default setup—all monitoring is performed by the local probe.

The Application core server inside the corporate LAN is able to monitor services and servers in the entire Local Area Network (LAN). Note: Core server and probe(s) are configured as Windows services which are permanently run by the Windows system without the requirement for a logged-in user.

In a cluster setup, a cluster probe runs on all nodes. There is an additional so-called Cluster Probe. All devices created on it are monitored by all nodes in the cluster, so data from different perspectives is available and monitoring for these devices always continues, also if one of the nodes fails.

Application automatically monitors system health of its own core server and of each probe in order to discover overloading situations that may distort monitoring results. To monitor the system status of the probe computer, Application automatically creates a few sensors. These include Core/Probe Health, Cluster Probe Health, Disk Free, and a bandwidth sensor for all installed network cards. We recommend keeping these sensors, but you can optionally remove all except the Health sensors. They measure various internal system parameters of the probe system hardware and the probe's internal processes and then compute a resulting value. Frequent or repeated values below 100% should be investigated.

A. Core Server:

The core server is the heart of your Application system and performs the following processes:

- Configuration management for object monitoring
- Management and configuration of the connected probes
- Cluster management
- Database for monitoring results
- Notification management including a mail server for email delivery
- Report generator and scheduler
- User account management
- Data purging (culling data that is older than 365 days, for example)
- Web server and API server

II. Literature Survey

Monitoring network traffic is not only for large businesses; it is something smaller networks can do as well. Monitoring your small businesses or family's network traffic has a lot of benefits and can reveal surprising results. It's best to have a basic understanding of networks and protocols before you begin to monitor your network traffic. Monitoring a computer on which System Monitor is running can affect computer performance slightly. Therefore, either log the System Monitor data to another disk (or computer) so that it reduces the effect on the computer being monitored, or run System Monitor from a remote computer. Monitor only the counters in which you are interested. If you monitor too many counters, resource usage overhead is added to the monitoring process and affects the performance of the computer that is being monitored concentrate your initial efforts in three main areas:

- Disk activity
- Processor utilization
- Memory usage

Using System Monitor, you can:

- View data simultaneously from any number of computers.
- View and change charts to reflect current activity, and show counter values that are updated at a frequency that the user defines.
- Export data from charts, logs, alert logs, and reports to spreadsheet or database applications for further manipulation and printing.
- Add system alerts that list an event in the alert log and can notify you by issuing a network alert.

- Run a predefined application the first time or every time a counter value goes over or under a user-defined value.
- Create log files that contain data about various objects from different computers.
- Append to one file selected sections from other existing log files to form a long-term archive.
- View current-activity reports, or create reports from existing log files.
- Save individual chart, alert, log, or report settings, or the entire workspace setup for reuse.

III. Background Methodologies

A. Probe Manager:

Application can track active protocols, IP addresses, number of packets and their size. User can easily track the workstations that download large volumes of data and identify that occupy bandwidth site. Application allows user to create their own list of hosts that want to monitor and displays the corresponding traffic statistics in a separate window.

Libraries helps to manage device tree, which are updated using the same scanning interval as your device tree, shows the same data monitoring, but so located that you want it. This is interesting if you want to display data in various ways, depending on the target group, or application. For example, you can create a library that provides an overview of all its sensors for monitoring bandwidth, regardless of what device they're running. Even with the help of the application user can compare objects, it helps to compare different graphs.

B. MAPS

Detailed map can be designed

- Maps for the network can be created with detail
- Creating a quick glance of your network, which can be displayed on the network operations center screens?
- Manage network overview
- Add important sensors for monitoring.
- Manage top lists for sensors.

C. Notifications:

Our application helps to notify about packets, traffic, protocols etc. even helps to solve the error. Alarm is set and triggers when defined value matches. Application send the notification when certain defined activity takes place, even the channels for notification are selected eg mails or sms etc.

- Sensor changes
- Sensor breach
- Speed breach
- Volume breach
- Value change

IV. Result

Application helps in network monitoring and overview packet movements and about source & destination. User can identify traffic issues and diagnoses network slow-downs. Application is very simple to use and gives real time statics about the activities. Application converts all the related statics in charts also so that monitoring is easier.

V. Conclusion

Even small companies can have complex computer networks that are a considerable investment. Multiple computers and servers, as well as routers and switches, are all interconnected and a problem in one can eventually spread throughout the network. One of the advantages of network management is that there is a system in place that can monitor every part on a constant basis; a problem with one component can be detected and resolved before most people even know about it. Network management often provides a means for security, access control, system upgrades, and policy enforcement.

Monitoring increases overall efficiency by saving time and reducing expenditures so that organizations can put their valuable resources elsewhere instead of manually tracking and compiling an inventory of a company's IT assets. With automated IT asset tracking software, all monitored computers in a network become visible in a single central console, providing organizations with real-time information they need in just a few clicks of a mouse, saving IT administrator's weeks of intensive work. Additionally, with remote monitoring, teams can share potential problems to address issues, resulting in better efficiencies and improved accuracy.

Reference

[1] http://www.naukrihub.com/recruitment/advantage-and-disadvantage-of-e-recruitment.html

[2] Know Advantages of E-Recruitment | Disadvantages of E-Recruitment

[3] http://en.wikipedia.org/wiki/Candidate_Submittal Candidate submittal - Wikipedia, the free encyclopedia

[4] http://en.wikipedia.org/wiki/Sourcing_(personnel) Sourcing (personnel) - Wikipedia, the free encyclopedia

[5] http://allsalesjob-info.blogspot.com/ sales Jobs

[6] http://en.wikipedia.org/wiki/Recruitment_process Recruitment - Wikipedia, the free encyclopedia