NSM Lab Assignment 1	
Name	Abhishek Mahajan
Class	Final Year CSE-NS
Roll No.	2183011

Aim – Discuss different Network Management Tools

Theory – Network management is the process of administering, managing, and operating a data network, using a network management system. Modern network management systems use software and hardware to constantly collect and analyze data and push out configuration changes for improving performance, reliability, and security.

The system manages network devices such as switches, routers, access points, and wireless controllers. It typically uses a centralized server to collect data from network elements. The server can be located on-premises, in a private data centre, or in the cloud.Devices, clients, and applications on the network can send data to the server with updates about their status. Network administrators can monitor network operations by logging in to the server, usually through a web browser or a smartphone app.

Network Monitoring Tool is an application that gathers useful information from different parts of the network. It will help in managing and controlling the network. The focus of network monitoring will be on performance monitoring, fault monitoring, and account monitoring.

It is used for examining the components like applications, email servers, etc. In order to examine the network or its internal components, it sends a signal or Ping to the various system ports.

Different Network Management Tools are as follows –

1. **SolarWinds Network Performance Monitor**
   SolarWinds Network Performance Monitor is a comprehensive network performance monitoring tool that can monitor the status of devices with SNMP. It can automatically discover network devices connected to your network.
   Key features:
   > SNMP monitoring
   > Automatically discovers connected network devices
   > Network packet analysis
   > Intelligent network maps with NetPath
   > Create WiFi heat maps
   > Custom Alerts system
   > Reports system

2. **Datadog Network Performance Monitoring**
   Datadog Network Performance Monitoring is a cloud-based SaaS infrastructure monitoring service that examines network traffic flows. It is partnered by a Network

Device Monitoring service, which focuses on the statuses of each device on the network, such as switches, routers, and appliances.
Key features:
- Live network mapping and protocol analysis
- Alerts on performance thresholds that are adjusted through machine learning
- Correlation with data from SNMP and other sources

The Datadog Network Performance Monitoring service begins its work by exploring your network and identifying each device. This autodiscovery service means all of the setup of the monitoring system is performed for you. The network discovery routine creates a device inventory, which forms an index for the entire monitoring service.

Once all devices and links have been identified, you can get an overview of all network activity from the Datadog dashboard. The service also draws up a network topology map and that can be used to get quick insights into each node or link. The map is clickable, creating a link through to device statistics and performance details. That information also extends to Internet connections out to other sites and cloud resources.

3. **ManageEngine OpManager**
   ManageEngine OpManager is a network monitoring solution that can monitor the performance of network devices, servers, routers, switches, and virtual machines in real-time.
   Key features:
   - Automatic discovery
   - Network mapping
   - SNMP monitoring
   - Email and SMS alerts
   - Customizable dashboards

4. **Auvik**
   Auvik is a cloud-based network monitoring system that includes a number of system management tools. The package is accessed through a Web browser and when you open an account, the setup process installs collectors on your system. The Auvik package is able to monitor multiple sites and centralizes their control. This makes the package ideal for monitoring a WAN.
   The service provided by Auvik begins with a network discovery process. This automatically populates all of the base information needed for the monitor to work. The discovery service is continuous, so it will spot when new devices are added to the network.

   Key features:
   - Automated setup
   - Network mapping

Resource utilization alerts

Configuration management

5. **Paessler PRTG Network Monitor**

PRTG Network Monitor from Paessler is a free network monitoring suite that uses SNMP, packet sniffing, and WMI to monitor your network. Scan network segments to discover and add devices to monitor. You can choose between a range of sensors to monitor various segments of your network. Each sensor monitors an individual value in your network, for instance, there are Bandwidth Monitoring Sensors, Hardware Parameters Sensors, network data usage meters, SNMP sensors, VOIP and QoS sensors, and more

Key features:

SNMP monitoring

Bandwidth monitoring

Scan for network devices by IP segment

Custom dashboards

Threshold-based alerts system

Reports system

Customizable network maps

For greater visualization, the tool has a customizable dashboard that allows you to produce real-time network maps of your infrastructure. You can create maps with the drag-and-drop editor and use over 300 map objects to build the map. You can even create your own map objects with custom HTML

Conclusion – Different NMS Tools have been studied and their different features are specified.

NSM Lab Assignment 2	
Name	Abhishek Mahajan
Class	Final Year CSE-NS
Roll No.	2183011

Aim – Analyze Network using Solar Winds Network Performance Monitor Tool.

Theory – SolarWinds is one of the world's leading producers of IT management software. The company's Network Performance Monitor (NPM) is one of its key products. This system focuses on monitoring the health of the devices connected to a network. The hardware that SolarWinds Orion NPM keeps an eye on includes network equipment, such as routers and switches; endpoint devices, including terminals, desktop PCs, and mobile devices; and office equipment, such as printers. The constant monitoring process gathers metrics that serve troubleshooting tasks.

Scanning of whole network with solarwinds
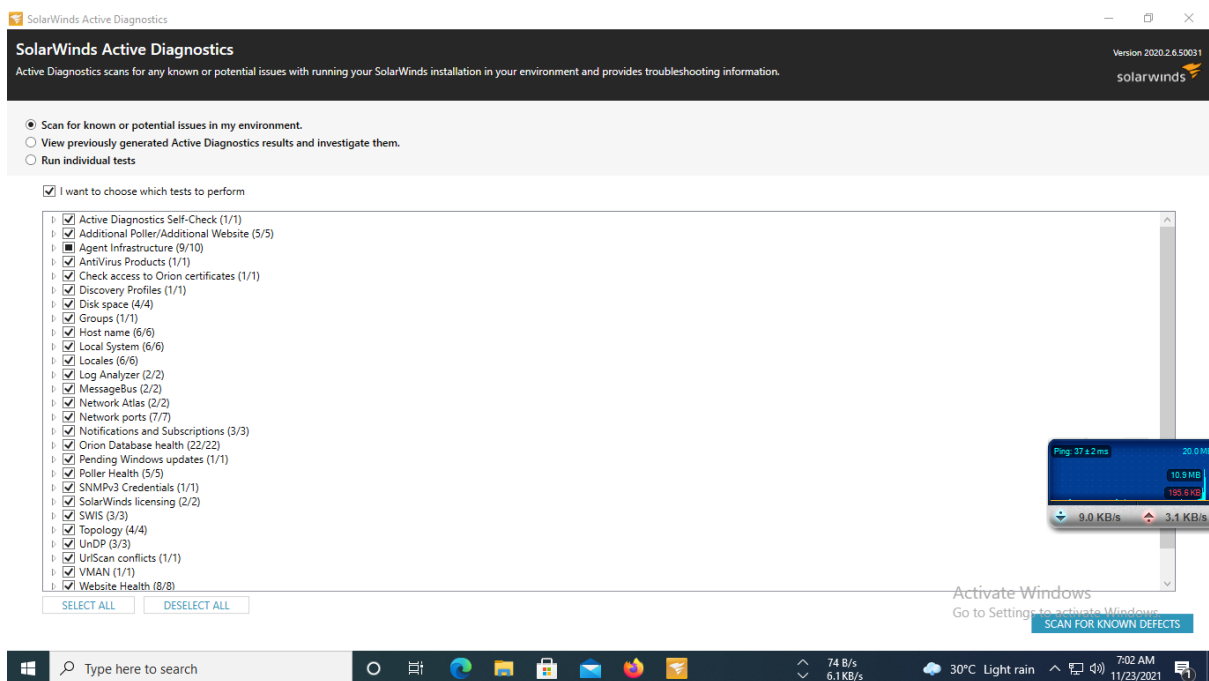
The above shows 3 options, and user can use any one to scan the network.

The list of the test can be seen the above image which helps to specify which test is been performed and be customized according to network checks.

Scan report-

Issues suggested/possible for network problem-

SolarWinds Active Diagnostics

Version 2020.2.6.50031

Active Diagnostics scans for any known or potential issues with running your SolarWinds installation in your environment and provides troubleshooting information.

solarwinds

Known issues

TITLE	DESCRIPTION
Polling completion (Poller Health)	Polling completion at engine LT105L is less than 92.00%. Polling completion is mostly impacted by CPU and memory resources so if polling completion significantly lower than 100% you should check your CPU and memory utilization. (Expand for more details)

Possible issues

TITLE	DESCRIPTION
Antivirus Products (AntiVirus Products)	Antivirus products are installed and enabled: Product Name: Windows Defender Is Running: True See KB: 2078. (Expand for more details)
Verify the optimization settings (Orion Database health)	Cost Threshold for Parallelism specifies when the SQL server creates and runs parallel plans for queries. The current value of Cost Threshold for Parallelism is '5', consider using 50 and adjust as necessary. Max Degree Of Parallelism (MAXDOP) specifies the number of processors used to execute a query in a parallel plan...
Identify pending Windows updates (Pending Windows updates)	The number of updates not installed is: 8. Your product may not install successfully. Ensure that pending Windows updates are installed if the installation fails. (Expand for more details)

TITLE: Identify pending Windows updates (Pending Windows updates)

DISCOVERED: 11/23/2021 7:07:26 AM

RESOLUTION: Ensure that pending Windows updates are installed if the installation fails.

DESCRIPTION: The number of updates not installed is: 8. Your product may not install successfully.

Check that SSLv2 connections are forbidden (Windows Security Infrastructure)	SSLv2 connections are not forbidden. Server is vulnerable for DROWN attack. Use the Windows Registry Editor to navigate to the following key: HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server Set Enabled value(DWORD) to 0. In case regi...

Ping: 38 ± 0 ms
20.0 MB
11.5 MB
456.7 KB
2.9 KB/s   74 B/s

Activate Windows
Show advanced view
Go to Settings to activate Windows.

RETURN TO START PAGE   EXPORT RESULTS   CLOSE

TITLE: Verify the optimization settings (Orion Database health)

DISCOVERED: 11/23/2021 7:07:15 AM

RESOLUTION: Cost Threshold for Parallelism specifies when the SQL server creates and runs parallel plans for queries. The current value of Cost Threshold for Parallelism is '5', consider using 50 and adjust as necessary. Max Degree Of Parallelism (MAXDOP) specifies the number of processors used to execute a query in a parallel plan. Use the number of physical cores in a single CPU socket. The current value of MAXDOP is '0', the re...
'4'.
Make sure the Query Optimizer Fixes setting is 'ON'.
See KB: OrionCoreAGDatabaseServerBestPractices.

Identify pending Windows updates (Pending Windows updates)	The number of updates not installed is: 8. Your product may not install successfully. Ensure that pending Windows updates are insta... (Expand for more details)
Check that SSLv2 connections are forbidden (Windows Security Infrastructure)	SSLv2 connections are not forbidden. Server is vulnerable for DROWN attack. Use the Windows Registry Editor to navigate to the following key: HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server Set Enabled value(DWORD) to 0. In case regi...

Ping: 38 ± 1 ms
20.0 MB
11.5 MB
456.7 KB
6.0 KB/s   3.4 KB/s

Activate Windows
Show advanced view
Go to Settings to activate Windows.

RETURN TO START PAGE   EXPORT RESULTS   CLOSE

○ Scan for known or potential issues in my environment.
○ View previously generated Active Diagnostics results and investigate them.
● Run individual tests

- ▷ Active Diagnostics Self-Check   Run tests
- ▷ Additional Poller/Additional Website   Run tests
- ▷ Agent Infrastructure   Run tests
- ▷ ⚠ AntiVirus Products   Run tests
- ▷ Check access to Orion certificates   Run tests
- ▷ Discovery Profiles   Run tests
- ▷ Disk space   Run tests
- ▷ Groups   Run tests
- ▷ Host name   Run tests
- ▷ Local System   Run tests
- ▷ Locales   Run tests
- ▷ Log Analyzer   Run tests
- ▷ MessageBus   Run tests
- ▷ Network Atlas   Run tests
- ▷ Network ports   Run tests
- ▷ Notifications and Subscriptions   Run tests
- ▷ ⚠ Orion Database health   Run tests
- ▷ ⚠ Pending Windows updates   Run tests
- ▷ ⛔ Poller Health   Run tests
- ▷ SNMPv3 Credentials   Run tests
- ▷ SolarWinds licensing   Run tests
- ▷ SWIS   Run tests
- ▷ Topology   Run tests
- ▷ UnDP   Run tests
- ▷ UrlScan conflicts   Run tests
- ▷ VMAN   Run tests

RUN ALL   EXPORT RESULTS

⛔ **Poller Health**

🟢 Check whether connection ports are exhausted by Agents

RESULT: Success

DURATION: 00:00:00.0011664

DISCOVERED: 11/23/2021 7:06:42 AM

DESCRIPTION: There are no connection port issues have found.

🟢 Check whether connection ports are exhausted by MS WMI issues

RESULT: Success

DURATION: 00:00:00.0192912

DISCOVERED: 11/23/2021 7:06:42 AM

DESCRIPTION: There are no connection port issues have found.

🟢 Element count

RESULT: Success

DURATION: 00:00:00.0583904

Activate Windows
Go to Settings to activate Windows.

Ping: 40 ± 2 ms   4.0 M
10.3 KB
↓ 2.0 KB/s   ↑ 74 B/s

Type here to search   0 B/s 1.6 KB/s   30°C Light rain   7:06 AM 11/23/2021

⚠ **Pending Windows updates**

⚠ Identify pending Windows updates

RESULT: Warning

DURATION: 00:00:08.4517778

DISCOVERED: 11/23/2021 7:06:35 AM

RESOLUTION: Ensure that pending Windows updates are installed if the installation fails.

DESCRIPTION: The number of updates not installed is: 8. Your product may not install successfully.

Ping: 38 ± 0 ms   4.0 M
125.1 KB
↓ 7.5 KB/s   ↑ 3.5 KB/s

Activate Windows
Go to Settings to activate Windows.

Type here to search   248 B/s 2.4 KB/s   30°C Light rain   7:06 AM 11/23/2021

Conclusion – Network is analysed using SolarWinds NPM and a report is generated.

NSM Lab Assignment 3	
Name	Abhishek Mahajan
Class	Final Year CSE-NS
Roll No.	2183011

Aim – Use Net Balancer tool to Control your traffic with priorities and rules

Theory – NetBalancer is an internet traffic control and monitoring tool designed for Microsoft Windows 7, 8 and 10

NetBalancer can be used for :

- Set a download and/or upload network **priority or limit** for any process

- Manage priorities and limits for each network adapter separately

- Define detailed network traffic rules

- Set global traffic limits

- Get detailed statistics and totals about your data usage

- Show network traffic in system tray

Dashboard –
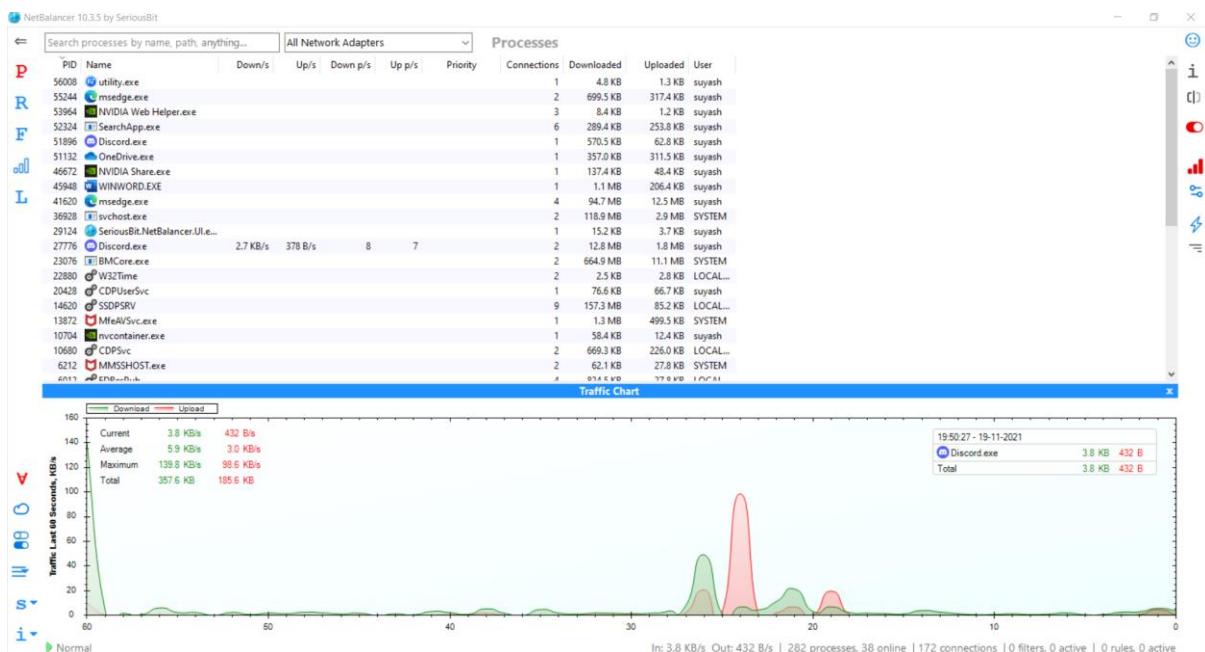
Rules creation (example msedge.exe) –

Priorities creation and list (example Discord.exe) –

Net Balancer also provides a Tray for monitoring network on the go –
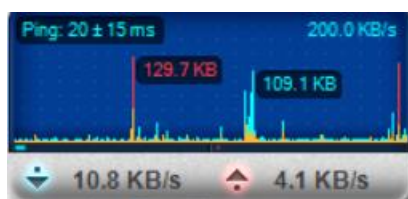
Conclusion – Net Balancer tool's uses is studied and is used to control the network with priorities and rules.

NSM Lab Assignment 4	
Name	Abhishek Mahajan
Class	Final Year CSE-NS
Roll No.	2183011

Aim – Use Paessler PRTG Network Monitor for monitoring and managing network nodes

Theory –

 PRTG monitors your entire IT infrastructure.

All-important technologies are supported:

• SNMP: ready-to-use and custom options

• WMI and Windows Performance Counters

• SSH: for Linux/Unix and macOS systems

• Traffic analysis using flow protocols or packet sniffing

• HTTP requests

• REST APIs returning XML or JSON

• Ping, SQL, and many more

Dashboard -
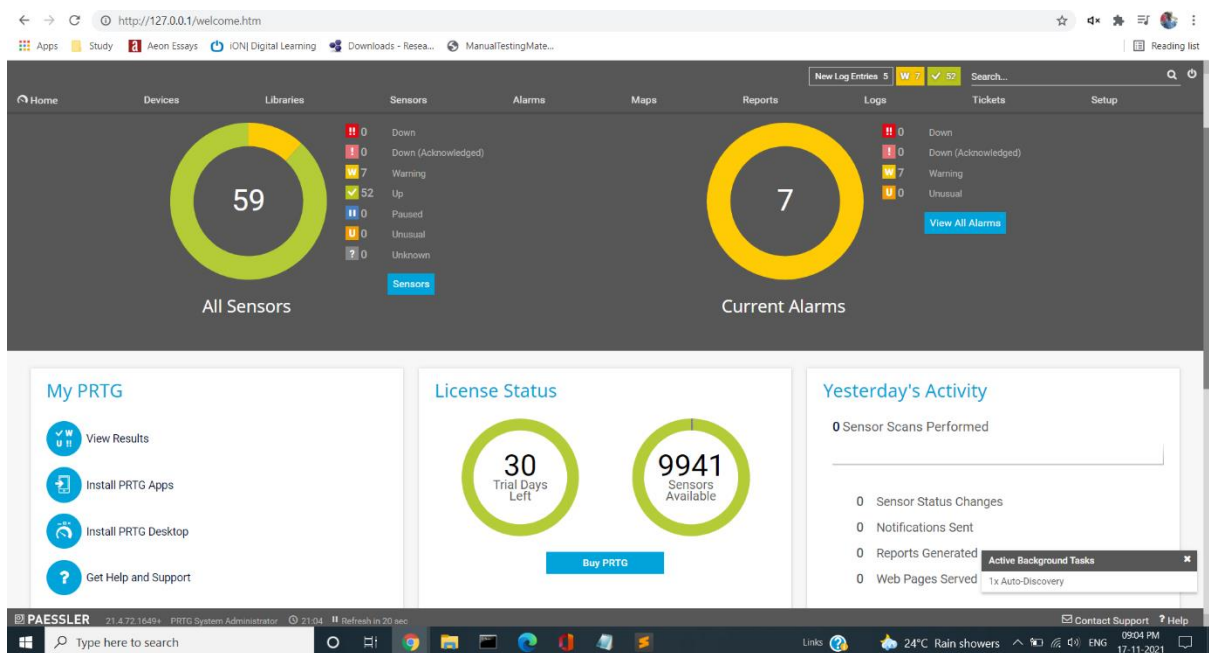
Group and devices on the network:
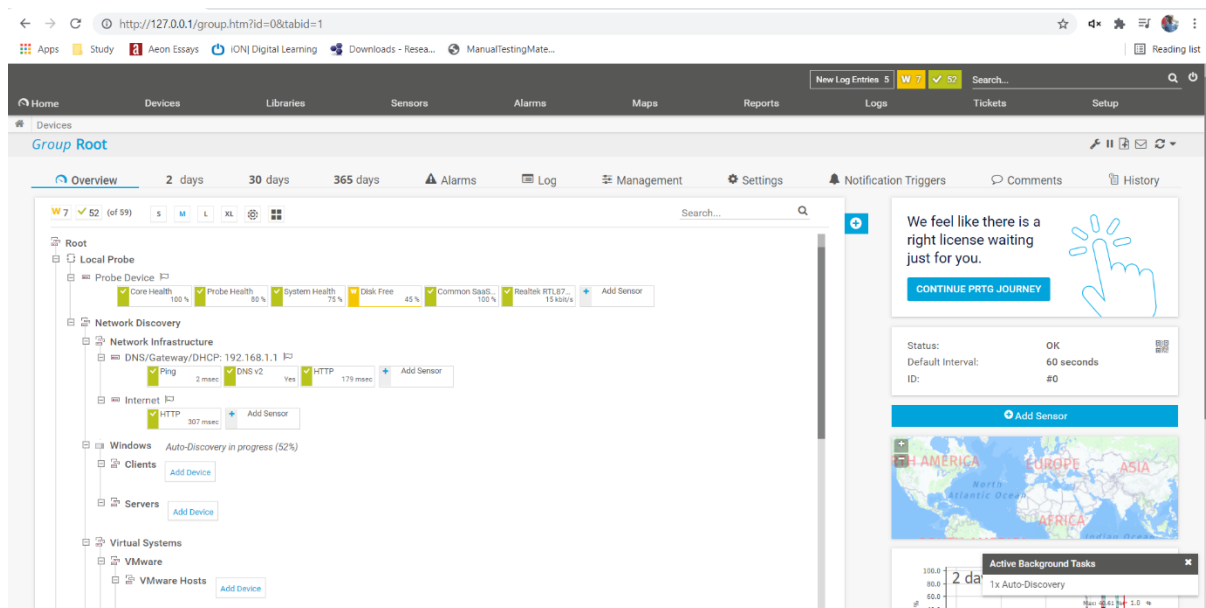
Sensor Disk report:
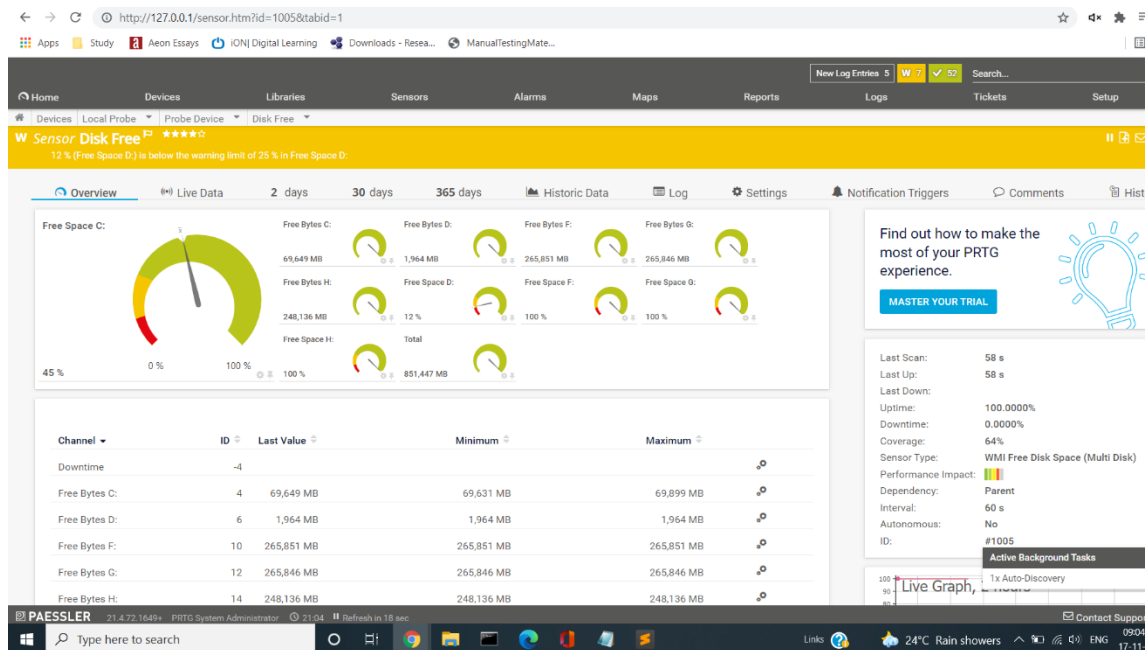
Core report about the Network:
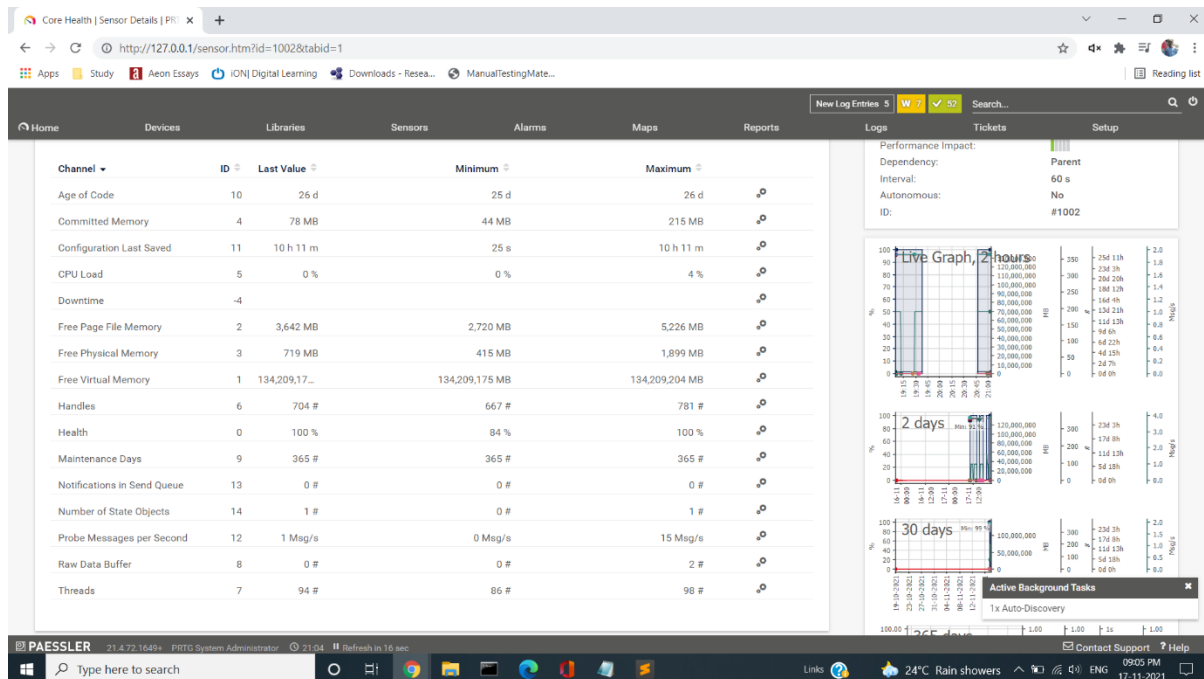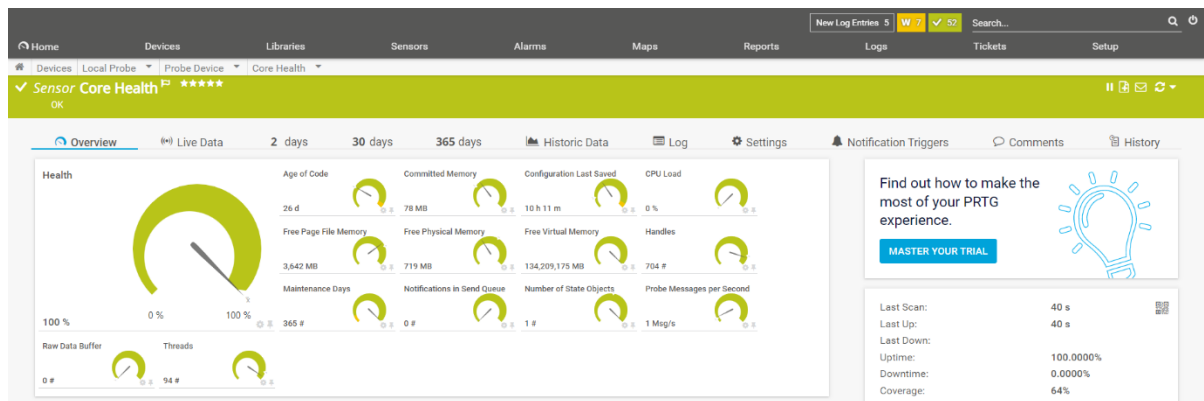
All the active sensor in the network with the ip address of the device:

IP address of the system:


```
Command Prompt
'ipcongfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\HP>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3dc8:30c5:e1b:8b2d%25
   IPv4 Address. . . . . . . . . . . : 10.0.2.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VirtualBox Host-Only Network #2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1d6a:ac07:a7f3:d935%17
   IPv4 Address. . . . . . . . . . . : 10.0.2.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : iballbatonwifi.com
   Link-local IPv6 Address . . . . . : fe80::3196:faff:8e3d:a3c0%18
   IPv4 Address. . . . . . . . . . . : 192.168.1.205
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

C:\Users\HP>
```

Conclusion – Paessler PRTG Network Monitor tool is used.

NSM Lab Assignment 5	
Name	Abhishek Mahajan
Class	Final Year CSE-NS
Roll No.	2183011

Aim – Use SoftPerfect Bandwidth manager for scaling and managing bandwidth need on network

Theory – SoftPerfect Bandwidth Manager is a full-featured traffic management tool for Windows that offers cost-effective bandwidth control and quality of service based on built-in prioritised rules. These rules can specify a bandwidth limit for each Internet user. The software of this kind is otherwise known as bandwidth limiter or traffic shaper. With its help, you can apply speed-throttling rules to specified IP and MAC addresses, ports and even network interfaces with no changes to your existing network infrastructure. The rich feature set of SoftPerfect Bandwidth Manager software is easily managed via the intuitive Windows GUI.

Key features

- Centralised configuration from a single network location.

- Flexible, prioritised, bidirectional rules to specify maximum data rates and usage allowances.

- Rules for IP and MAC addresses, protocols, ports (for TCP/IP) and network interfaces.

- Transparency for end users with no client software installation required in most cases.

- Quotas, scheduler, email notifications and comprehensive usage reports

Dashboard –
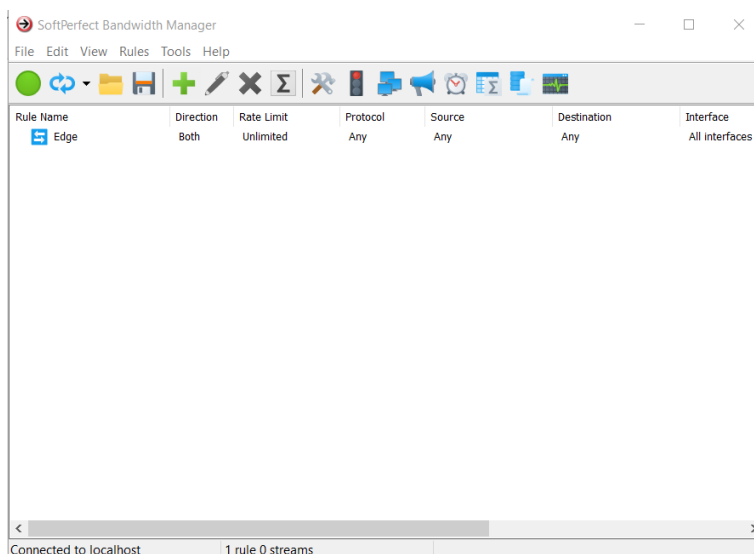
Rule –
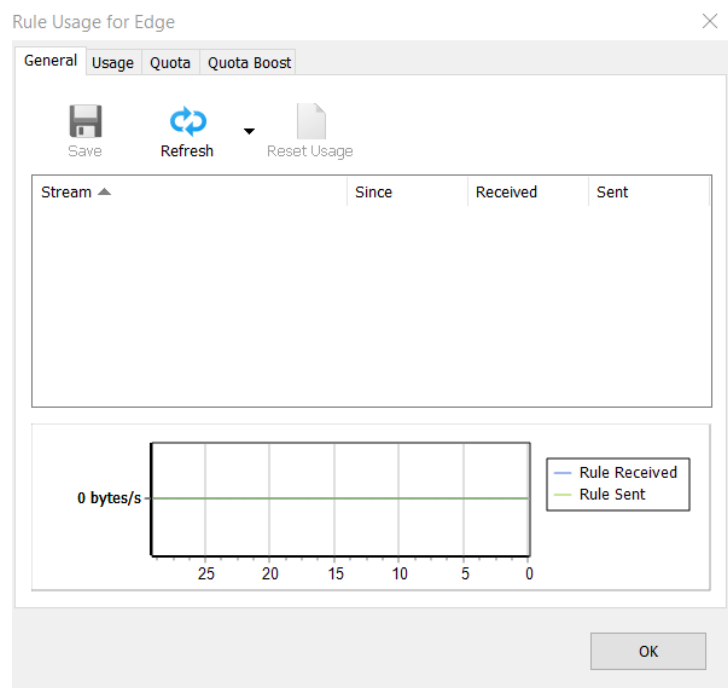
Conclusion – Bandwidth Manager is used for creating rules for scaling and managing Bandwidth.

NSM Lab Assignment 6	
Name	Abhishek Mahajan
Class	Final Year CSE-NS
Roll No.	2183011

AIM: Study Assignment on Zabbix.

Theory:

Zabbix is an open source monitoring software tool for diverse IT components, including networks, servers, virtual machines (VMs) and cloud services. Zabbix provides monitoring metrics, such as network utilization, CPU load and disk space consumption. The software monitors operations on Linux, Hewlett Packard Unix (HP-UX), Mac OS X, Solaris and other operating systems (OSes); however, Windows monitoring is only possible through agents.

Zabbix can be deployed for agent-based and <u>agentless</u> monitoring. Agents are installed on IT components to check performance and collect data. The agent then reports back to a centralized Zabbix management server. That information is included in reports or presented visually in the Zabbix graphical user interface (<u>GUI</u>). If there are any issues regarding what is being monitored, Zabbix will send a notification or alert to the user. Agentless monitoring accomplishes the same type of monitoring by using existing resources in a system or device to emulate an agent.

The Zabbix web-based GUI enables users to view their IT environment via customizable dashboards based on <u>widgets</u>, graphs, network maps, slideshows and reports. For example, a user can customize a report to show metrics associated with both service-level agreements (<u>SLAs</u>) and key performance indicators (<u>KPIs</u>) on CPU loads.

Zabbix offers several monitoring features:

- Simple checks can verify the availability and responsiveness of standard services such as SMTP or HTTP without installing any software on the monitored host.
- A Zabbix agent can also be installed on UNIX and Windows hosts to monitor statistics such as CPU load, network utilization, disk space, etc.
- As an alternative to installing an agent on hosts, Zabbix includes support for monitoring via SNMP, TCP and ICMP checks, as well as over IPMI, JMX, SSH, Telnet and using custom parameters. Zabbix supports a variety of near-real-time notification mechanisms, including XMPP.

Released under the terms of GNU General Public License version 2, Zabbix is free software
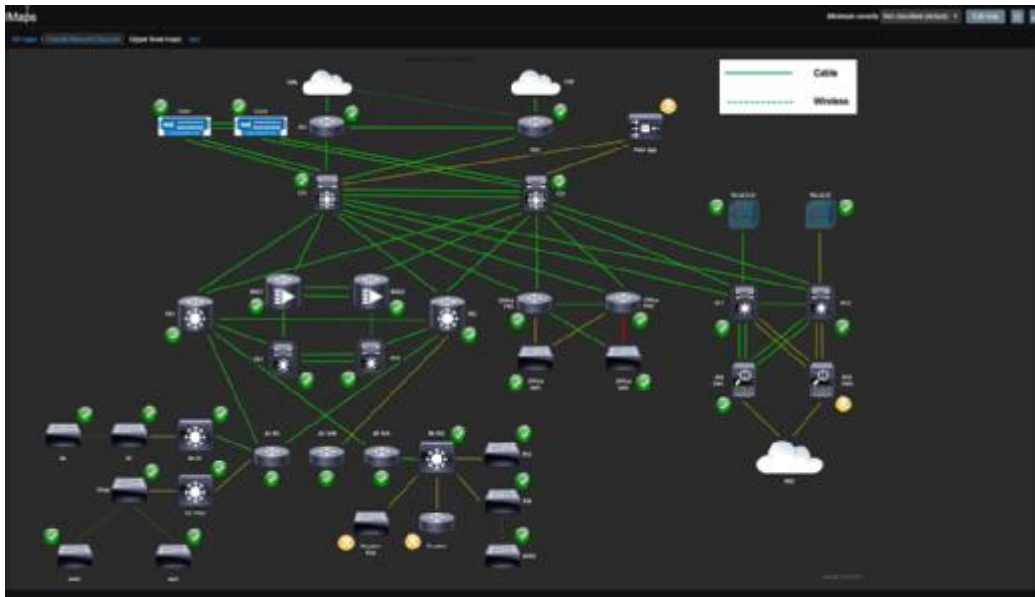
This map shows the connections Zabbix forms among machines, servers and a cloud service.

Zabbix works via three discovery mode options:

- **Network discovery** periodically scans an IT environment and records a device's type, IP address, status, uptimes and downtimes.

- **Low-level discovery** automatically creates items, triggers and graphs based on the discovered device. Low-level discovery can create metrics from Simple Network Management Protocol (SNMP) object identifiers, Windows services, Open Database Connectivity (ODBC) Structured Query Language (SQL) queries, network interfaces and more.

- **Auto-discovery** automatically starts monitoring any discovered device using a Zabbix agent.

With Zabbix distributed monitoring, remotely run scripts collect data from multiple devices in distributed locations and combine that data in one dashboard or report, such as server availability across the country.
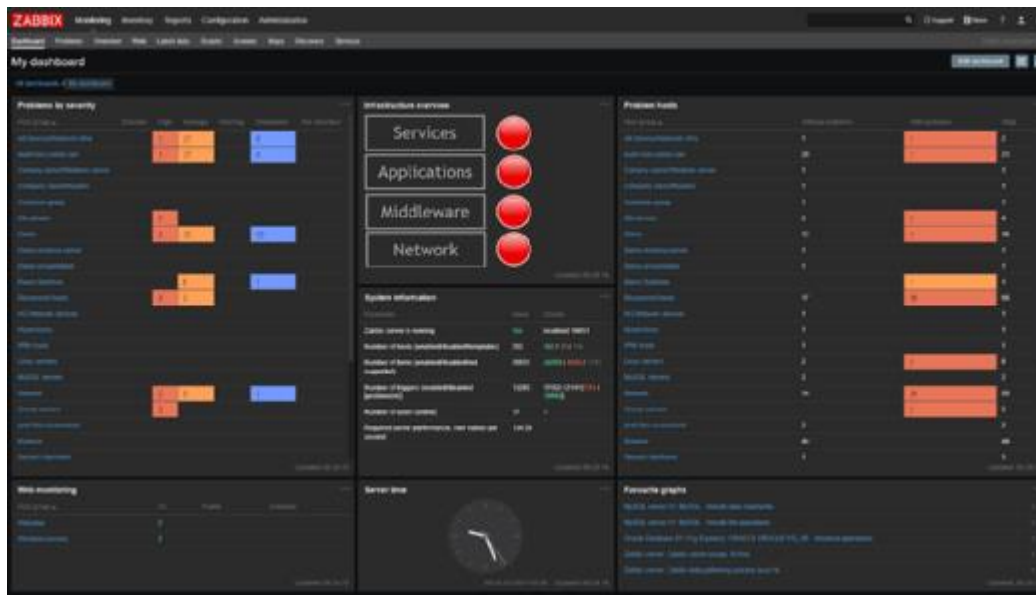
Zabbix's GUI offers data points that range from system health to error severity and location, as well as monitoring details.

Zabbix can send email notifications based on predefined events in a user's IT environment. Another way for Zabbix users to stay up to date with their IT environment is through mobile applications from suppliers such as M7 Monitoring or of their own creation.

Agentless monitoring options with Zabbix

Zabbix offers several monitoring options beyond agents.

A simple check can verify the availability and responsiveness of a standard service, such as notifications, or HTTP.

Java management extensions (JMX), web monitoring and other methods are also alternatives to using agents. In Zabbix, JMX can be used to monitor Java-based applications. Web monitoring is used to check the availability of websites and supports HTTP and HTTPS. Zabbix collects data relating to the average download speed of a scenario, errors and error messages, response time and more.

The Zabbix API

The Zabbix application programming interface is a web-based API to create new applications, automate tasks and integrate with third-party software, such as go-zabbix, Zabbix::Tiny or Zabbix sender. The JavaScript Object Notation (JSON) format is used to base the API as a front-end web interface.

The Zabbix API consists of many methods that are grouped together into separate APIs, each performing a specific service. For example, a method to create a new host is host.create; the method to log in as an admin is user.login.

Utilizing the API, users can create applications to work with and display Zabbix information.

Templates for additional monitoring capabilities

Templates are custom-built add-ons that extend the functionality of Zabbix. Some templates are made by Zabbix and come packaged with the software ready for use, while others are built by Zabbix users. Templates enable Zabbix users to monitor network devices from vendors such as Cisco, Dell, HP and Juniper. Other templates can be used to monitor IBM, HP and Super Micro servers. Templates for application-based services include Microsoft Exchange and Exchange Server, Zenoss, PowerDNS, Authoritative Server Stats and more. Templates can be created to monitor OSes and hypervisors as well.

Infrastructure monitoring competitors to Zabbix

Microsoft System Center Operations Manager (SCOM), Nagios and Zenoss are examples of competing IT infrastructure monitoring systems.

SCOM enables configuration, management and monitoring for an IT ecosystem through one management console. SCOM can monitor server hardware, system services, OSes, hypervisors and applications, similar to Zabbix. SCOM also uses agent-based and agentless monitoring similar to Zabbix.

Nagios is another open source monitoring program for IT environments. Nagios can monitor Linux, Unix and Windows OSes. Nagios offers multiple products, such as Core, XI, Log Server, Network Analyzer and Fusion. Nagios can run active checks that are self-initiated and run passive checks that are completed using external applications. Nagios uses both agent-based and agentless monitoring as well.

Zenoss is monitoring software available in three forms: Zenoss Core, Zenoss Service Dynamics and Zenoss as a Service (ZaaS). Zenoss Core is the open source version of the software, which contains the basic components of the monitoring software. Core also can be used to create ZenPacks, Zenoss' equivalent to templates. Zenoss Service Dynamics is the on-premises version of the software, which can monitor IT infrastructures, such as servers,

networks and databases. ZaaS is delivered as software as a service (SaaS) with the same monitoring capabilities as Service Dynamics.

Features:

High performance, high capacity (able to monitor hundreds of thousands of devices).

- Auto-discovery of servers and network devices and interfaces.
- Low-level discovery automatically starts monitoring new items, file systems or network interfaces among others.
- Distributed monitoring with centralized web administration.
- Native high-performance agents (client software for Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X, Tru64/OSF1, Windows 2000, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008, Windows 7).
- SLA, and ITIL KPI metrics on reporting.
- High-level (business) view of monitored resources through user-defined visual console screens and dashboards.
- Remote command execution through Zabbix proxies since August 2017, up to Zabbix 3.4.
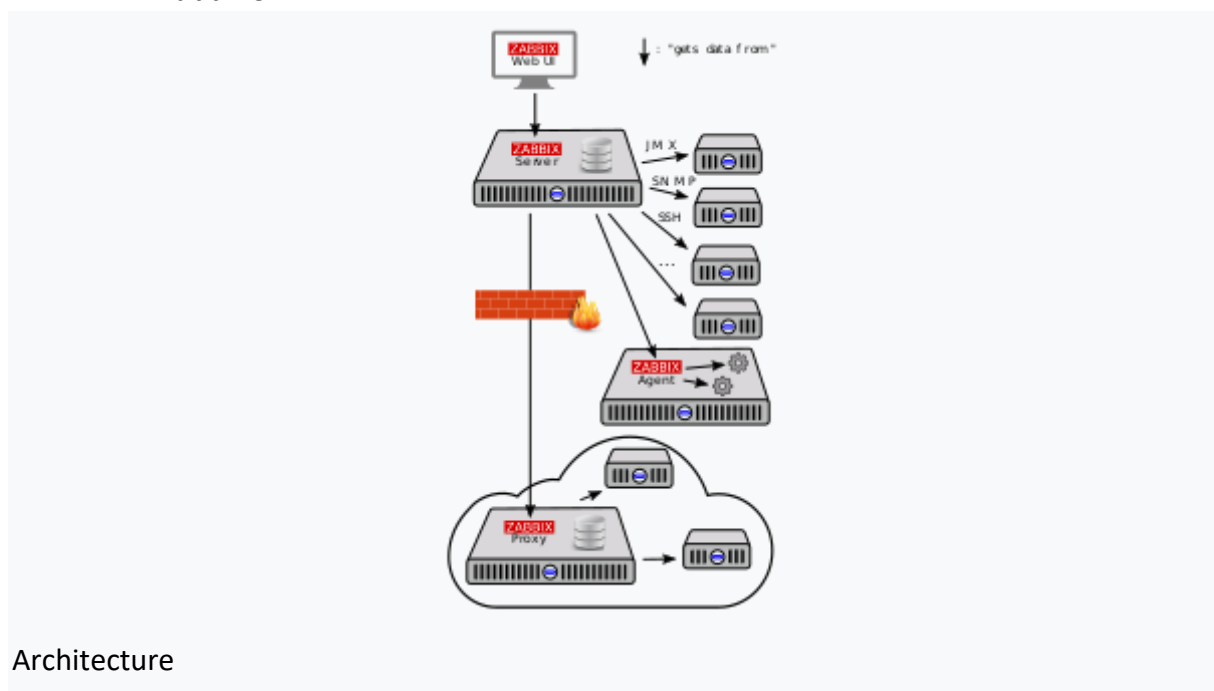
Architecture

Architecture

- Agent or Agent-less monitoring capabilities.
- Web-based interface.
- Support for both polling and trapping mechanisms.

Monitoring

- JMX monitoring.

- Web monitoring.

Security and authentication

- Audit log.
- Secure user authentication.
- Flexible user permissions.

Notification capabilities

- Flexible e-mail notification on predefined events.
- Near-real-time notification mechanisms, for example using including XMPP protocol.

Lets See some CASE STUDY based on the some of the experience of user who used Zabbix in their organization.

#CASE STUDY 1:

How Bank of China Uses a Scale-Out Database to Support Zabbix Monitoring at Scale

Bank of China is the fourth largest state-owned commercial bank in China. Since 2016, we've been using Zabbix, a popular open-source monitoring solution, to monitor our IT infrastructure. We used to use MySQL as the backend storage for Zabbix; however, MySQL is not scalable enough to monitor IT environments on a large scale. After trying different solutions, we chose TiDB, a MySQL-compatible, open-source, distributed SQL database to replace MySQL as the backend for a large-scale Zabbix. With TiZabbix, we successfully monitor more than 10,000 hosts and query 18 TB of monitoring data.

In this blog post, I will first introduce the traditional Zabbix monitoring solution we adopted and our pain points at the time. Then, I will give a detailed look at how we use TiDB in Zabbix. Finally, I will share our further plans to optimize TiZabbix.

#CASE STUDY 2:

How MakeMyTrip Monitors Its Large-Scale E-Commerce Website

MakeMyTrip, an online travel company, talks about their monitoring philosophy and setup in a series of articles. The hybrid infrastructure is monitored across the stack by mostly open source tools.The first two articles cover system, network and application monitoring, and some insights into the monitoring pipeline itself. MakeMyTrip's infrastructure is spread out over datacenters, public and private clouds and comprise both bare metal as well as virtual machines. The key tools are Zabbix for alerting, a 6-stage pipeline for collecting, aggregating and storing metrics built out of open source tools like OpenTSDB, Kafka, Elasticsearch and Grafana along with some home grown ones.

#CASE STUDY 2:

Miyazaki Prefectural Government Office Case Study Interview

In the application of the Miyazaki Prefecture server integration infrastructure, QTNet used "Zabbix" as its monitoring solution. Zabbix 2.2 is used to provide monitoring of the operational status of the server groups and network devices that form this integrated infrastructure, with monitoring data always available to be checked via a portal.

Monitoring is an important aspect of virtual infrastructure just as it is with physical servers. Mr. Katsuaki Kozu, IT basic technology section System development 1 division at Densan Software Co.,Ltd. states: "We organize things by making duplicates or triplicates of systems using virtualization technology so that there is no problem even if one system drops out. We have use Zabbix to prepared a setup that quickly grasps and escalates any occurrence."

There were various alternative monitoring tools, including software for business use, but Zabbix was top of the list as it satisfied Miyazaki Prefecture's requirements and could facilitate cost reduction. "It wasn't down to whether the software was open source or not, but rather it was a question of finding software that would satisfy the monitoring requirements," says Mr. Toshiyuki Munakata, Operating Officer and Head of the Corporate Sales Department at Kyushu Telecommunication Network Co., Inc. (QTNet).

Conclusion: Thus, we get to know different features and important points about the Zabbix in NMS.