20) Network Monitoring

Sunday, December 01, 2024 5:51 PM

SNMP(Simple Network Management Protocol):
It is a network management protocol for **TCP/IP**

Components of SNMP:
It is basically made up of three main components **Managed Devices, SNMP Manager** and **SNMP Agent**

Managed Devices:
Printers, Workstations, etc

SNMP Agent:
Software which runs on managed devices

SNMP Manager:
Request and processes information from the agent software. Also known as **Network Management System(NMS)**

SNMP uses mainly 8 different kind of PDUs(Protocol Data Units) for querying and responding to the managed devices. Four of them are:

Get:
Sending **GetRequest** or **GetNextRequest** for the query

Response:
Agent responds to the query

Set:
If there needs a change in the query response, NMS sends **SetRequest**

Trap:
A trap is basically a notification/alert sent by the managed device irrespective of any query made

Net-SNMP package in Linux contains a command called **snmpwalk** which is for troubleshooting SNMP related issues. SNMP has three versions, SNMPv1, SNMPv2c and SNMPv3

NOTE that SNMP categorizes data using **MIB(Management Information Base)**, depending upon the type/format of data being queried

SNMP protocol is **UDP** on port **161 and 162**. With TLS, ports are **10162 and 10161**

Monitoring Tools:

Packet Sniffer:
A program that queries a NIC and stores all the captured packets in a file called **Capture File**. These programs can run on computers, dedicated hardware or routers etc. A packet sniffer is usually connected to a **mirrored port**

Protocol Analyzers:
It is a program for reading the **Capture File**. It performs **packet/traffic** analysis like IP and MAC of a packet etc.

NOTE: Filtering in Wireshark is a very good paying skill

NetFlow:
It is basically a tool for monitoring, developed by Cisco. It is based on the idea of the type of flow we want to track

- A **flow** is a sequence of packets from one specific place to another. These flow are stored in a **Flow Cache**

Top Talkers are the devices sending the most data and **Top Listeners** are the opposite

Sensors:
For controlling things like temperature, device/chassis etc.

Interface Monitors:
Tracks the bandwidth and utilization of ports in a network. Some of the terms that can be seen in a interface monitor are: Link State, Speed/Duplex, Send/Receive Traffic, CRC Errors, Protocol Packet and Byte Counts, Giants, Runts, Encapsulation Errors, Uptime/Downtime etc.

Performance Monitors:
It basically tracks the performance for some part of the OS like how much the web server is putting, etc. **Syslog** is a tool in Linux and **perfmon** is a tool in Windows

Logs:
These are basically the system log file to track performance

Baselines:
It is basically a baseline for as to how the optimal network should perform so that if networks breaks down or boosts up, the baseline could be compared

Log Management:
The log files should be secured and managed well. The protection and management of it is called **Log Management**

Log files are **cyclical**, means that if they grow to a certain size, the older ones are deleted. **Also, there are many laws according to which the log files should be kept for a certain period of time**

Putting It All Together:

Monitoring and Managing:
A centralized location for tech and admins to manage the network in an environment is called **NOC(Network Operations Center)**. Some of the tools used are **Cacti, Grafana, Zabbix, SolarWinds, etc.**

SIEM(Security Information and Event Managment):
It is basically a term used for calling out monitoring and management of network. It is made-up of two different processes, **SEM(Security Event Managment) and SIM(Security Information Management)**.

SEM:
It is the real-time monitoring of security events and saving them in a single viewing point say, a log file. What is also does is that it centralizes the other security monitors and event logs

SIM:
It reviews and analyzes log file things like file size, configuration values, content, credentials, hash values etc. Are seen as to what changes have been made and usually compared to the baseline. This is also known as **File Integrity Monitoring(FIM)**. These are either self-implemented or managed by an admin under contract by **Managed Security Service Provider(MSSP)**