Network Scanning, Monitoring, and Patching

by Sophia

WHAT'S COVERED

In this lesson, you will learn about techniques for identifying potential network problems that may need troubleshooting.

Specifically, this lesson will cover:

1. Logging

Logging is the act of gathering, storing, processing, synthesizing, and analyzing data from various networks and systems. Log data is then used to manage and optimize performance, identify problems, and manage resources in order to support high availability, robust security, and regulatory compliance.

TERM TO KNOW

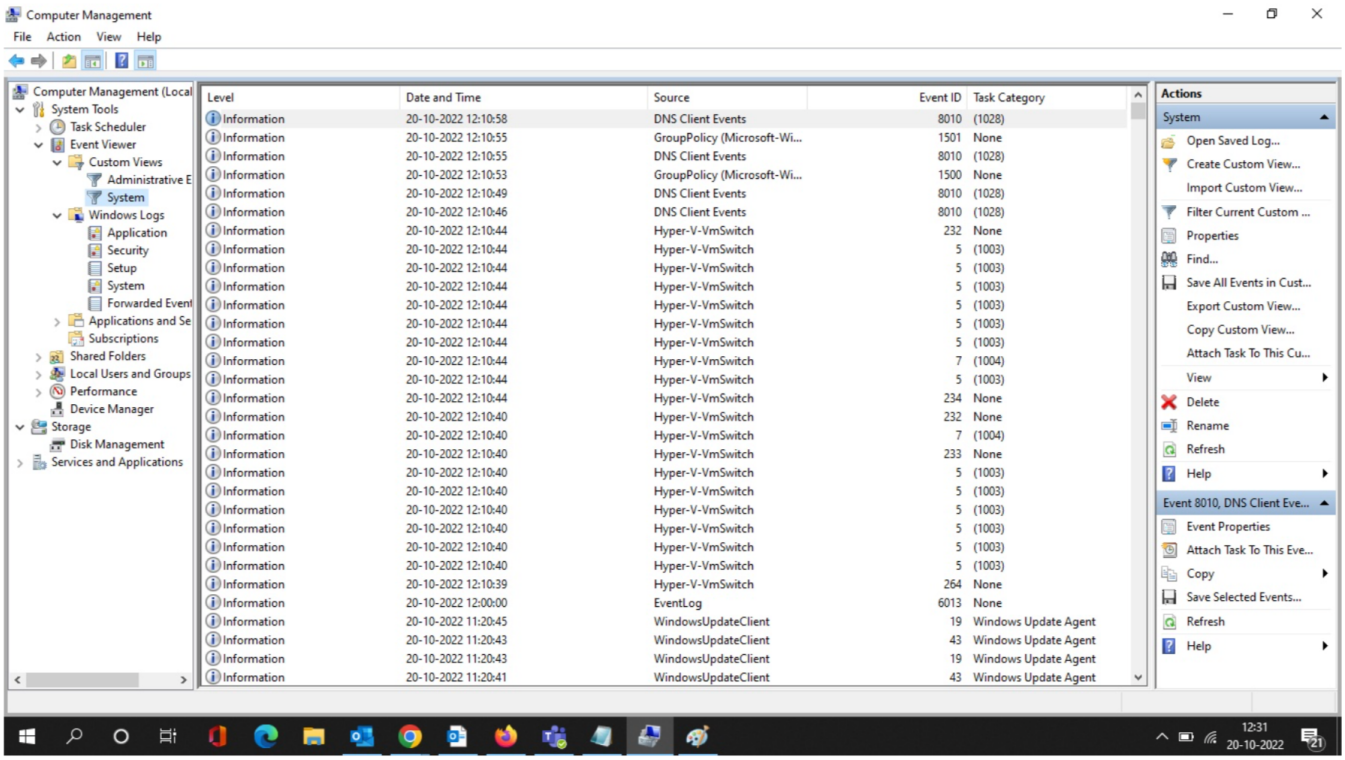
Logging

An act of gathering, storing, processing, synthesizing, and analyzing data from various networks and systems.

1a. Log Reviewing

The Event Viewer utility, available in most Windows versions, provides several logs containing vital information about events happening on your computer. Other server operating systems have similar logs, and many connectivity devices like routers and switches also have graphical logs that gather statistics on what's happening to them. These logs can go by various names, like history logs, general logs, or server logs.

The screenshot below shows an Event Viewer system log display from a Windows Server machine.



KEY CONCEPT

On Windows servers, a minimum of three separate logs hold the following types of information:

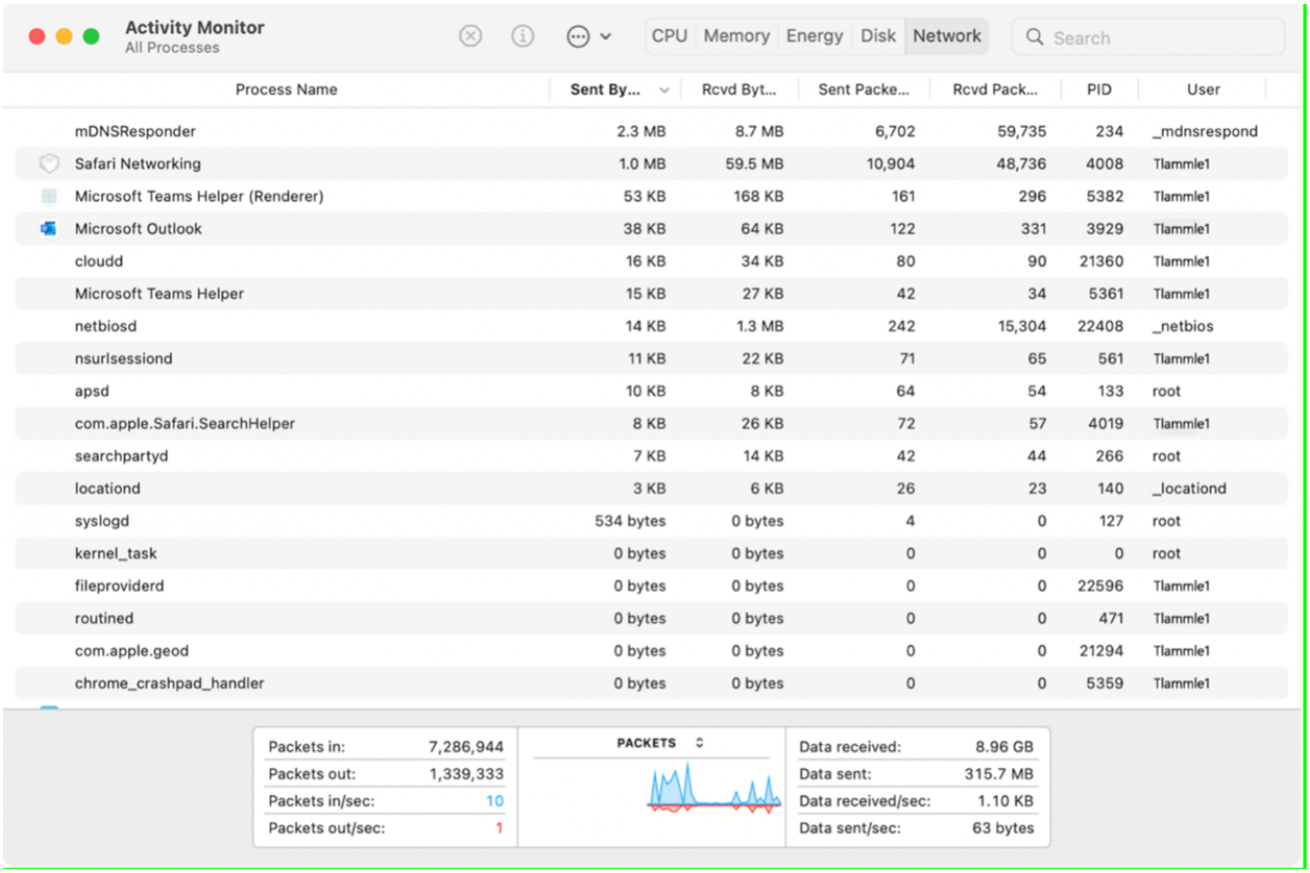
- Application: Contains events triggered by applications or programs determined by their programmers. Example applications include LiveUpdate, the Microsoft Office suite, and SQL and Exchange servers.
- Security: Contains security events like valid or invalid log-on attempts and potential security problems.
- System: Contains events generated by Windows system components, including drivers and services that started or failed to start.

These three basic types of logs can give us a lot of information about who is logging on, who is accessing the computer, and which services are running properly (or not). If you want to find out whether your Dynamic Host Configuration Protocol (DHCP) server started up its DHCP service properly, just check out its system log. Because the computer depicted above is configured as a domain controller, its Event Viewer serves up three more logs: Directory Service, DNS Server, and File Replication Service, for a total of six logs.

1b. Bandwidth Utilization

Wired and wireless analyzers can log data about the bandwidth used on your network segments or wireless service set. There are also tools to help you find the stats on storage, network devices, CPU, and device memory logged by your servers and hosts.

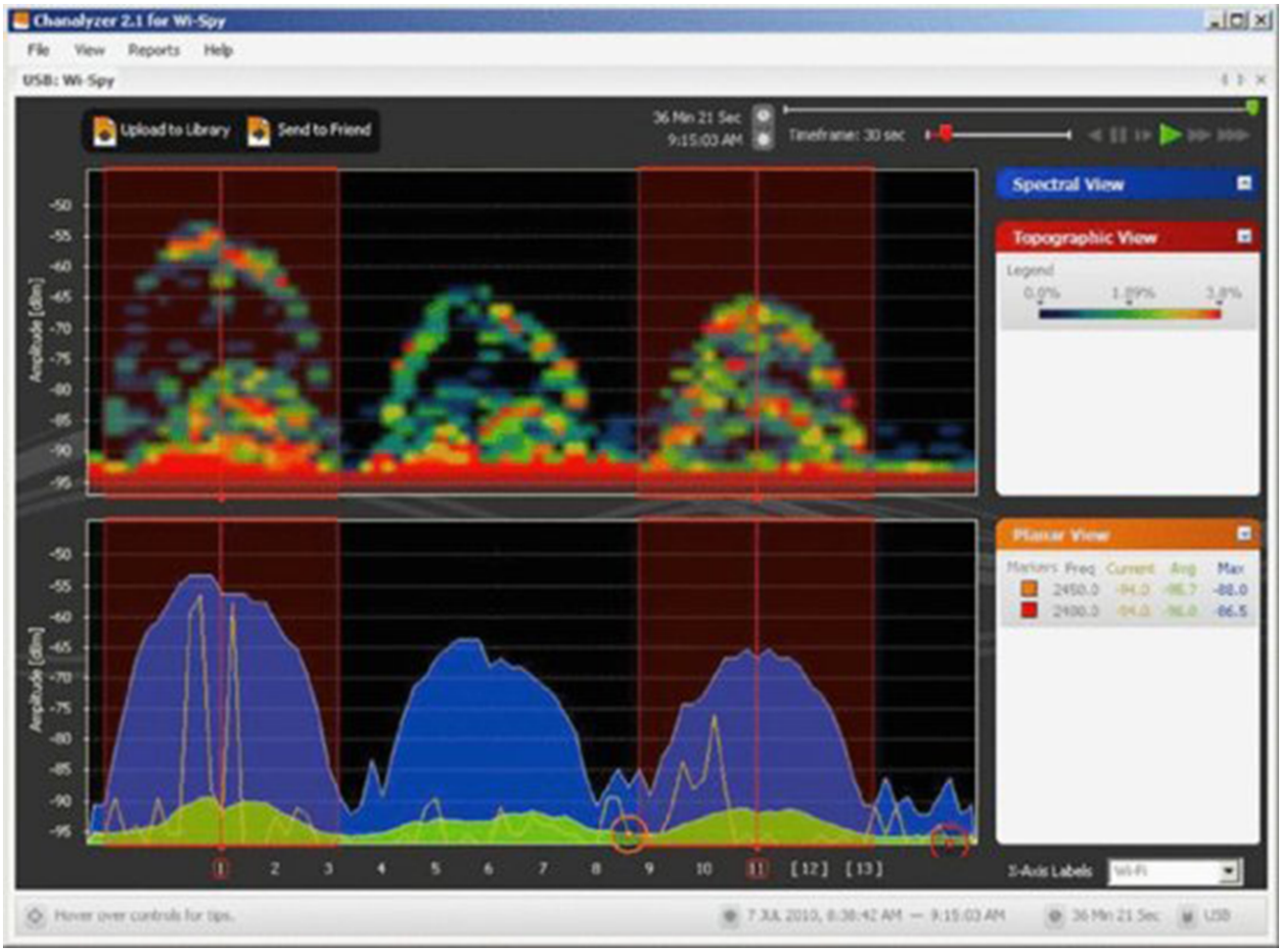
> EXAMPLE If you have a Mac, you can use the built-in activity monitor, which provides the CPU usage, memory statistics, energy used by the applications, disk usage, and network bytes sent and received, as shown in the screenshot below.



In addition to utilization information for your hosts, servers, networks, and so on, you need information about the wireless channel utilization on your network.

HINT

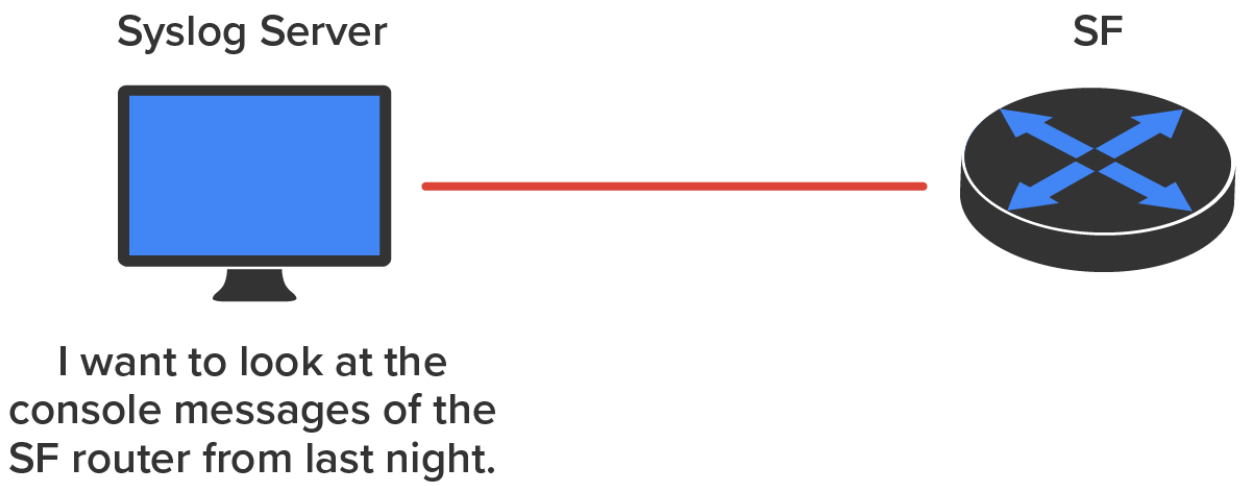
To get it, you need to use a wireless analyzer. The wireless analyzer below shows channel utilization. Notice that three channels—1, 6, and 11—are in use.



1c. Syslog

Reading system messages from a switch's or router's internal buffer is the most common and efficient method of seeing what's going on with your network at a particular time. But the best way is to log messages to a **syslog** server, which stores messages from you and can even timestamp and sequence them for you.

EXAMPLE The diagram below shows a syslog server and client in action.



KEY CONCEPT

Syslog enables you to display, sort, and even search messages, all of which makes it a really great troubleshooting tool. The search feature is especially powerful because you can use keywords and even severity levels. Plus, the server can email administrators based on the severity level of the message.

TERMS TO KNOW

Syslog
A standard network logging protocol.

2. Scanning

Scanning is the act of inspecting, analyzing, or examining various aspects of networks or systems with the intention of checking for problems. For example, the device you are using now is likely configured to scan its storage components for errors so that the operating system can fix them. Likewise, network administrators periodically do scans of network resources to look for problems.

TERM TO KNOW

Scanning
An act of inspecting, analyzing, or examining, various aspects of networks or systems with the intention of checking for problems.

2a. Port Scanning

A **port scanner** is a software tool designed to search a host for open ports. Network administrators use port scanners to test network security, and hackers use them to find a network's vulnerabilities and compromise them.

KEY CONCEPT

A **vulnerability** is a weakness that allows an attacker to reduce a system's security.

To **port scan** means to scan for Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) open ports on a single target host. The scan helps a user to connect to and use its services for business and/or personal reasons. Port scanning is also used maliciously to locate and connect to ports to attack the host and steal information.

In contrast, **port sweeping** means scanning multiple hosts on a network for a specific open TCP or UDP port. This is a favorite approach hackers use when trying to invade your network. They port sweep in a broad manner, and then, if they find something—in this case, SQL—they can port scan the particular host they have discovered with the desired service available to exploit and get what they are after.

HINT

This is why it is best practice to turn off any unused services on your servers and routers and to run only the most essential services on every host machine in your network. Make sure your security policy requires this mitigation.

A **SYN scan** is the most popular form of TCP scanning. Rather than using the operating system's network functions, the port scanner actually generates raw IP packets and monitors for responses. This scan type is also known as half-open scanning because it never really opens a full TCP connection. The port scanner generates a SYN packet, and if the targeted port is open, it will respond with a SYN-ACK packet. The scanner host responds with an RST (reset) packet, closing the connection before the handshake is completed.

TERMS TO KNOW

Port Scanner

A software tool designed to search a host for open ports.

Vulnerability

A weakness which allows an attacker to reduce a system's security.

Port Scan

A scan for TCP and UDP open ports on a single target host.

Port Sweeping

Scanning multiple hosts on a network for a specific open TCP or UDP port.

SYN Scan

A technique used to determine the state of a TCP or UDP port without fully opening a connection to it.

3. Monitoring

A basic tenet of business culture is the idea that if you can't measure it, you can't manage it. Monitoring and measuring network and system performance characteristics is crucial to our ability to quantify metrics that

enable data-driven decision making about how to manage our information technology infrastructure. Developing baselines is a key step in network monitoring that supports effective and efficient troubleshooting.

3a. Reviewing Baselines

High-quality documentation should include the baseline for network performance, because you and your client need to know what "normal" looks like in order to detect problems before they develop into disasters. It is also important to verify that the network conforms to all internal and external regulations and that you have developed and itemized effective management procedures and security policies for future network administrators to refer to and follow.

In networking, a **baseline** can refer to the standard level of performance of a certain device or to the normal operating capacity for your entire network. For instance, a specific server's baseline describes norms for factors like how busy its processors are, how much of the memory it uses, and how much data usually goes through the network interface card (NIC) at a given time.

KEY CONCEPT

A network baseline indicates the amount of bandwidth available and when. For networks and networked devices, baselines include information about four key components:

- Processor
- Memory
- Hard-disk (or other storage) subsystem
- Wired/wireless network utilization

After everything is up and running, it is a good idea to establish performance baselines on all vital devices and your network in general. To do this, measure things like network usage at three different strategic times to get an accurate assessment. For instance, peak usage usually happens around 8:00 a.m. Monday through Friday, or whenever most people log in to the network in the morning. After hours or on weekends is often when usage is the lowest. Knowing these values can help you troubleshoot **bottlenecks** or determine why certain system resources are more limited than they should be. Knowing what your baseline is can help you determine whether someone's complaints about the network running slowly are valid.

Some server operating systems come with software to help with network monitoring, which can help find baselines, manage logs, and even graph network usage so you can compare the logs and graphs at a later time to check for changes.

It is wise to re-baseline network performance at least once a year. And always pinpoint new performance baselines after any major upgrade to your network's infrastructure.

TERMS TO KNOW

Baseline

Data used as the basis for calculation or for comparison.

Bottleneck

A point of a network that is too slow or congested.

3b. Packet/Traffic Analysis

Protocol analyzers, also called sniffers or network monitors, are used to capture packets in their raw format as they cross the network. Wireshark is a protocol analyzer for Windows that you can download for free. Commercial sniffers like Wireshark and Omnipeek can capture any packets because they set the NIC to operate in promiscuous mode, which means the NIC processes all packets that it sees.

Protocol analyzers can be used to determine the type of traffic that you have in your network, and depending on the product and the bells and whistles contained therein, you may be able to sort the results based on port numbers, protocols, and so on. Another use of a **sniffer** is to examine the traffic that should be occurring on the network when something is not working to aid in troubleshooting. These devices can capture and display all packets involved in the connection setup, including, for example, request and response headers to a web server.

TERMS TO KNOW

Protocol Analyzer

A software or hardware tool for intercepting and logging network traffic.

Sniffer

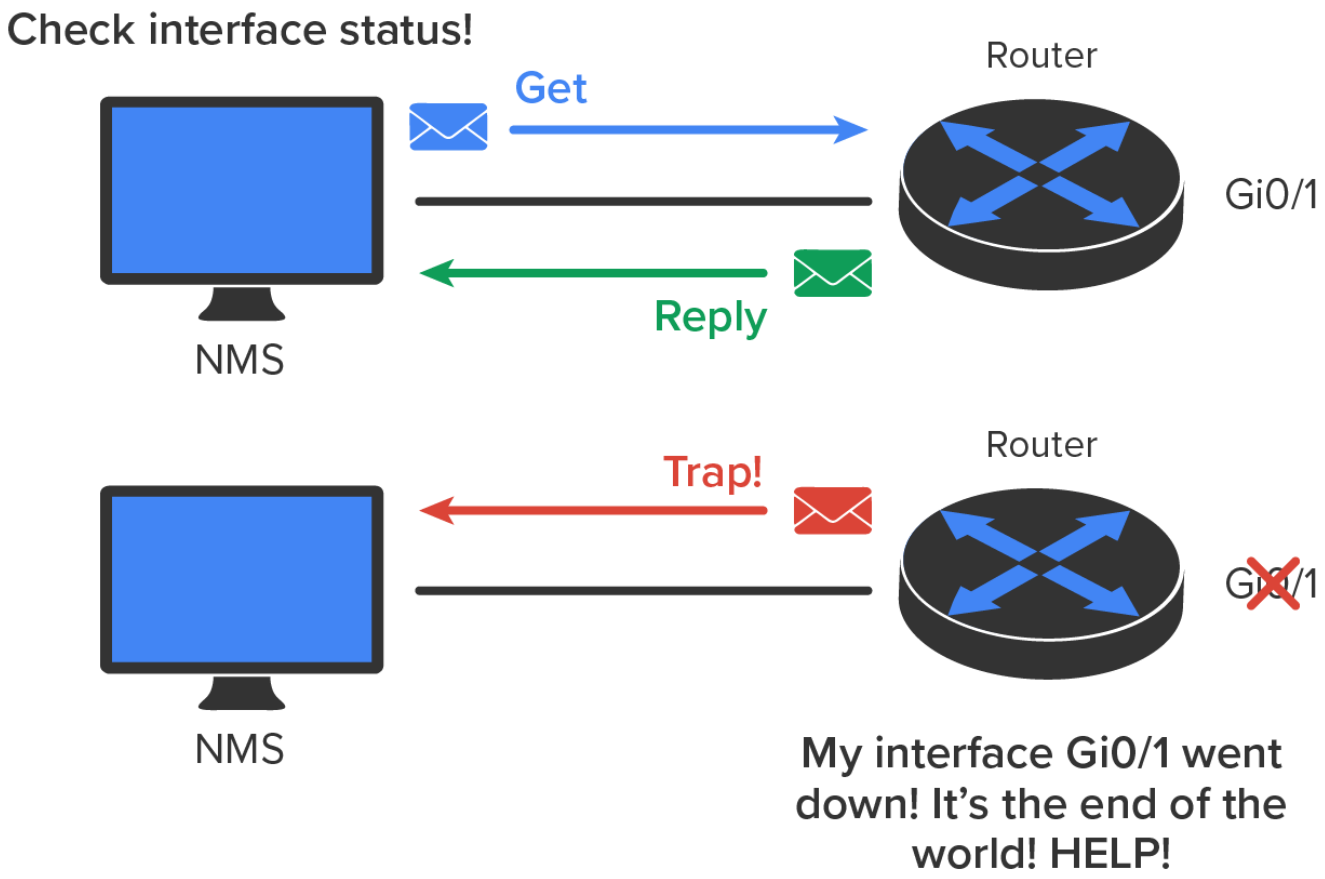
A software or hardware tool for intercepting and logging network traffic.

3c. SNMP Monitors

Simple network management protocol (SNMP) is a Layer 7 (Application) protocol that provides a message format for agents on a variety of devices to communicate with a **network management station (NMS)**. These agents send messages to the NMS station, which then either reads or writes information in the Management Information Base (MIB), a database stored on the NMS.

The NMS periodically queries or polls the SNMP agent on a device to gather and analyze statistics via GET messages. These messages can be sent to a console or alert you via email or SMS. The command snmpwalk uses the SNMP GET NEXT request to query a network for a tree of information.

An endpoint device running SNMP agents will send an SNMP trap to the NMS if a problem occurs. This is demonstrated below:



Network administrators use SNMP to provide some configurations to agents. This is referred to as SET messages. In addition to polling to obtain statistics, SNMP is used to analyze information and compile the results in a report. Thresholds are used to trigger a notification process when exceeded. Graphing tools are used to monitor the CPU statistics of devices like a core router. The CPU should be monitored continuously, and the NMS can graph the statistics. Notifications are sent when an established threshold set has been exceeded.

KEY CONCEPT

SNMP has three versions, with version 1 being a legacy protocol. Here is a summary of these three versions:

- SNMPv1: Supports plaintext authentication with community strings (passwords) and uses only UDP.
- SNMPv2: Supports plaintext authentication with MD5 or SHA with no encryption, but provides GET BULK, which is a way to gather many types of information at once and minimize the number of GET requests. It offers a more detailed error message reporting method, but it is not more secure than v1. It uses UDP even though it can be configured to use TCP.
- SNMPv3: Supports strong authentication with MD5 or SHA, providing confidentiality (encryption) and data integrity of messages via DES or DES-256 encryption between agents and managers. GET BULK is a supported feature of SNMPv3, and this version also uses TCP.

TERMS TO KNOW

Simple Network Management Protocol (SNMP)

A Layer 7 (Application) protocol that provides a message format for agents on a variety of devices to communicate with a network management station (NMS).

Network Management Station (NMS)

A computer running a network management application.

3d. Security Information and Event Management (SIEM)

Security information and event management (SIEM) technology provides centralized real-time analysis of security alerts generated by network hardware and applications. You can get this as a software solution or a hardware appliance, and some businesses sell managed services using SIEM. Any one of these solutions can provide a log of security data and generate reports for compliance purposes.

SIEM can collect useful data about the following items:

- Data aggregation
- Correlation
- Alerting
- Dashboards
- Compliance
- Retention
- Forensic analysis

HINT

SIEM systems not only assess the aggregated logs in real time, but they generate alerts or notifications when an issue is discovered. This allows for continuous monitoring of the environment in a way not possible with other log centralization approaches such as syslog.

TERM TO KNOW

Security Information and Event Management (SIEM)

Technology that provides centralized real-time analysis of security alerts generated by network hardware and applications.

SUMMARY

In this lesson, you learned about techniques for identifying potential network problems that may need troubleshooting, including **logging, scanning**, and **monitoring**. We covered some fundamentals of log reviewing, bandwidth utilization, syslog, port scanning, vulnerability scanning, reviewing baselines, packet analysis, SNMP, and security information and event management.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Baseline
Data used as the basis for calculation or for comparison.

Bottleneck
A point of a network that is too slow or congested.

Logging
An act of gathering, storing, processing, synthesizing, and analyzing data from various networks and systems.

Network Management Station (NMS)
A computer running a network management application.

Port Scan
A scan for TCP and UDP open ports on a single target host.

Port Scanner
A software tool designed to search a host for open ports.

Port Sweeping
Scanning multiple hosts on a network for a specific open TCP or UDP port.

Protocol Analyzer
A software or hardware tool for intercepting and logging network traffic.

SYN Scan
A technique used to determine the state of a TCP or UDP port without fully opening a connection to it.

Scanning
An act of inspecting, analyzing, or examining, various aspects of networks or systems with the intention of checking for problems.

Security Information and Event Management (SIEM)
Technology that provides centralized real-time analysis of security alerts generated by network hardware and applications.

Simple Network Management Protocol (SNMP)
A Layer 7 (Application) protocol that provides a message format for agents on a variety of devices to communicate with a network management station (NMS).

Sniffer
A software or hardware tool for intercepting and logging network traffic.

Syslog

A standard network logging protocol.

Vulnerability

A weakness which allows an attacker to reduce a system's security.