**19CSE301-COMPUTER NETWORKS**

**SERVER HEALTH MONITORING SYSTEM**

|  |  |  |
| --- | --- | --- |
| **Roll no** | **Name** | **Role** |
| CB.EN.U4CSE21034 | MANTHINI MEHER VARDHAN |  |
| CB.EN.U4CSE21040 | NERELLA GEETHA KRISHNA |  |
| CB.EN.U4CSE21062 | TANGUDU HARSHA VARDHAN |  |

**Problem definition:**

"Developing a Server Health Monitoring System to continuously track and assess the performance, availability, and resource utilization of servers in real-time."

**Motivation for a Server Health Monitoring System:**

There are several compelling motivations for implementing a Server Health Monitoring System:

**Increased uptime and availability:** Servers are critical components of any IT infrastructure, and their uptime is crucial for business continuity. A comprehensive monitoring system can help detect and resolve issues before they cause outages, leading to increased uptime and availability.

**Improved performance:** Server performance directly impacts user experience and business productivity. By proactively monitoring key metrics like CPU usage, memory consumption, and disk space, administrators can identify bottlenecks and implement corrective actions to ensure optimal performance.

**Enhanced resource utilization:** A health monitoring system can help identify underutilized servers and allocate resources more effectively. This can lead to cost savings and improved overall system efficiency.

**Reduced downtime and data loss:** Timely detection of server issues can prevent them from escalating into major failures that result in downtime and data loss. This can save businesses significant time and money.

**Proactive and preventative maintenance**: By monitoring trends and identifying potential problems early, proactive maintenance can be scheduled to prevent costly downtime and data loss.

**Improved security:** Server health monitoring can help detect suspicious activity and security vulnerabilities, allowing administrators to take corrective action and mitigate the risk of cyberattacks.

**Reduced operational costs:** By automating monitoring tasks and reducing the need for manual intervention, server health monitoring systems can help reduce operational costs.

**Improved decision-making:** By providing comprehensive data and insights into server health, a monitoring system can assist administrators in making informed decisions about resource allocation, capacity planning, and future investments.

**Compliance:** Many industries have compliance regulations that require organizations to monitor their IT infrastructure. A server health monitoring system can provide the necessary data and reporting to demonstrate compliance.

**Improved collaboration:** By providing a central repository for server health data, a monitoring system can facilitate collaboration among different IT teams, leading to more efficient problem resolution.

**Scalability:** As organizations grow, their server infrastructure must scale accordingly. A server health monitoring system can be scaled to accommodate additional servers and provide a holistic view of the entire IT environment.

**Peace of mind**: Knowing that your servers are being monitored and that any potential issues will be quickly identified and addressed can give administrators peace of mind and allow them to focus on other tasks.

**Server Health Monitoring System Architecture:**

A typical server health monitoring system consists of several key components arranged in a layered architecture:

1**. Data Collection Layer:**

* Agents: These are software programs installed on each server to collect local performance data such as CPU usage, memory consumption, disk space, network traffic, application logs, and system events.
* Sensors: Hardware devices attached to servers that directly measure physical parameters like temperature, humidity, and fan speed.
* Data Acquisition Tools: Tools like SNMP and WMI are used to gather data from various sources.

2. **Data Aggregation Layer:**

* Middleware: This software component collects data from agents and sensors, performs initial processing and filtering, and aggregates it into a common format.
* Data Queue: A temporary storage location for data that is being processed and forwarded to the next layer.

**3. Data Management Layer:**

* Database: Stores historical performance data for long-term analysis and trending.
* Time-series Database: Optimized for storing and querying time-series data like server metrics.

**4. Data Analysis and Reporting Layer:**

* Analytics Engine: Analyses the collected data to identify trends, anomalies, and potential problems.
* Alerting Engine: Triggers alerts based on predefined thresholds and sends notifications to administrators.
* Reporting Engine: Generates reports that provide insights into server health and performance.
* Dashboard: Provides a visual representation of key performance indicators (KPIs) and server status.

**5. User Interface Layer:**

* Web Console: Enables administrators to view dashboards, reports, alerts, and configuration settings.
* Mobile App: Provides access to server health information on the go.

**Routing techniques:**

Static routing is a simple routing technique where a network administrator manually configures the routing table of routers in a network. Unlike dynamic routing protocols (e.g., OSPF or BGP), where routers exchange information to dynamically determine the best path for packets, static routing relies on manually configured routes that do not change unless modified by the administrator.

**Proposed algorithms:**

**“OSPF (Open Shortest Path First)**” is a routing protocol commonly used in networking to find the best path for data packets in a network

**1. Detecting Network Issues:**

OSPF routing tables can be monitored for changes in topology or path costs. This can help identify network issues that may impact server performance, such as link failures or congestion. By analyzing changes in routing tables and correlating them with other server metrics, administrators can gain valuable insights into the health of the network and its impact on server performance.

**2. Optimizing Data Collection:**

OSPF routing information can be used to optimize the collection of server health data. By understanding the network topology and the paths taken by data packets, administrators can strategically place monitoring agents and sensors to collect data efficiently and minimize network traffic overhead.

**3. Enhancing Alerting Systems:**

OSPF routing information can be integrated with server health monitoring systems to trigger alerts based on network conditions. For example, if OSPF detects a link failure that may impact server connectivity, the monitoring system can trigger an alert and initiate corrective actions, such as rerouting traffic or activating failover mechanisms.

**4. Identifying Security Threats:**

OSPF routing information can be used to identify suspicious network activity and potential security threats. By analysing unusual routing patterns or changes in routing metrics, administrators can identify potential malicious activity targeting servers or the network infrastructure.

**5. Planning and Capacity Management:**

OSPF routing information can be used to plan future network infrastructure upgrades and capacity expansions. By analysing the network traffic patterns and understanding server locations, administrators can utilize OSPF to determine the optimal placement of new servers and network equipment to ensure efficient performance and scalability.

**STP, HSRP, and VTP in Server Health Monitoring Systems:**

STP, HSRP, and VTP are network protocols primarily used for managing network topology and redundancy, but they can also play a supporting role in server health monitoring systems. Here is a breakdown of their contribution:

**STP (Spanning Tree Protocol):**

* Ensures loop-free network topology, preventing network instability and outages that could impact server performance.
* Monitoring STP transitions and troubleshooting any errors can help identify potential network issues that may affect server health.
* By understanding STP topology changes, server health monitoring systems can optimize data collection and communication paths for improved performance.

**HSRP (Hot Standby Router Protocol):**

* Provides redundancy for network gateways, ensuring high availability and minimizing downtime for servers.
* Monitoring HSRP state changes and identifying failed or degraded routers can help prevent server outages and ensure consistent network connectivity.
* By integrating HSRP information with server health data, administrators can gain a holistic view of the network health and its impact on server performance.

**VTP (VLAN Trunking Protocol):**

* Manages VLAN configuration across network devices, simplifying network administration and facilitating efficient network segmentation.
* Monitoring VTP updates and ensuring consistency across the network helps prevent configuration errors that could disrupt server communication and performance.
* By understanding VTP configuration, server health monitoring systems can track server traffic across different VLANs and identify potential performance bottlenecks.

Overall, STP, HSRP, and VTP play a crucial role in ensuring network stability and redundancy, which are essential for optimal server health and performance. By integrating these protocols with server health monitoring systems, administrators can gain valuable insights into the overall health of their IT infrastructure and proactively address potential issues.

* Here are some specific examples of how each protocol can be used in a server health monitoring system:

**STP:**

* + Identify loops in the network that could lead to instability and impact server performance.
  + Monitor STP transitions to ensure that they are happening smoothly and that servers are not experiencing connectivity issues during the transition.
  + Optimize data collection by routing traffic over the most efficient path based on the STP topology.

**HSRP:**

* + Identify failed or degraded routers that could lead to outages and impact server availability.
  + Ensure that servers are automatically switched to the backup router in the event of a failure, minimizing downtime.
  + Track the health of the backup router to ensure that it is ready to take over if needed.

**VTP:**

* + Identify VLAN configuration errors that could disrupt server communication and performance.
  + Monitor VLAN membership changes to ensure that servers are assigned to the correct VLANs for optimal performance and security.
  + Use VTP information to track server traffic across different VLANs and identify potential bottlenecks.

By leveraging these protocols, server health monitoring systems can be more comprehensive and effective, allowing administrators to proactively identify and address potential problems before they impact server performance and availability.

**Explanation of Layer Protocols in Server Health Monitoring System :**

**Physical Layer:**

* **Fast Ethernet:** This protocol offers data transfer rates of 100 Mbps. It's a common and reliable option for connecting servers and network devices.
* **Gigabit Ethernet:** This protocol provides significantly higher speeds (1 Gbps), making it ideal for high-bandwidth applications and large data transfers.
* **Serial Cables:** These cables are used for point-to-point communication between devices. They offer reliable data transmission over long distances.

**Data Link Layer:**

* **STP (Spanning Tree Protocol):**Ensures a loop-free network topology, preventing network instability and outages that could impact server performance.
* **VTP (VLAN Trunking Protocol):** Simplifies VLAN configuration and ensures consistency across network devices, facilitating efficient network segmentation.
* **EtherChannel (LACP, PAGP):** Combines multiple physical links into a single logical link, increasing bandwidth and redundancy for critical server connections.

**Network Layer:**

* **HSRP (Hot Standby Router Protocol):**Provides redundancy for network gateways, ensuring high availability and minimizing downtime for servers.
* **OSPF (Open Shortest Path First):** Optimizes network routing by finding the shortest paths between servers and network resources, leading to improved performance.

**Application Layer:**

* **HTTP (Hypertext Transfer Protocol):** This is the foundation of web communication, allowing servers to deliver content and applications to user devices.
* **DNS (Domain Name System):** Translates human-readable domain names into numerical IP addresses, enabling network devices to locate and connect to specific servers.

**Transportation Layer:**

* **TCP (Transmission Control Protocol):**Ensures reliable data delivery between devices by providing error checking, sequencing, and flow control.

This combination of protocols provides a comprehensive and reliable foundation for server health monitoring system. Each layer plays a critical role in ensuring efficient communication, data exchange, and network stability, ultimately contributing to effective server health monitoring and management.

Here's a brief explanation of each protocol's role in the server health monitoring system:

* **Physical Layer:** Establishes the physical connection between devices and transmits raw data.
* **Data Link Layer:** Encapsulates data into frames, adds error detection and correction mechanisms, and manages network access.
* **Network Layer:**Routes data packets across the network based on logical addressing and optimizes routing paths.
* **Transport Layer:** Provides reliable data transfer between applications running on different servers.
* **Application Layer:** Enables communication between applications and servers, such as web browsing, file transfer, and remote access.

**physical layer methodologies :**

In the context of a Server Health Monitoring System, the physical layer methodologies primarily focus on the physical network infrastructure and the technologies that facilitate the transfer of data between servers and networking equipment. Here are some physical layer methodologies relevant to a Server Health Monitoring System:

**Network Redundancy:**

Implementing physical redundancy in the network infrastructure is crucial for server health monitoring. This includes redundant switches, routers, and network links to ensure continuous connectivity even if a network component fails. Redundancy helps prevent single points of failure that could impact the availability of the monitoring system.

**High-Speed Ethernet Connections:**

Deploying high-speed Ethernet connections, such as Fast Ethernet (100 Mbps) or Gigabit Ethernet (1 Gbps), ensures fast and efficient data transfer between servers and the monitoring infrastructure. This high bandwidth is essential for handling the monitoring data generated by servers.

**Physical Security:**

Ensuring physical security of networking equipment and servers is a critical consideration. Unauthorized access to network devices or servers could compromise the integrity of the monitoring system. Implementing measures such as access controls, surveillance, and secure server room environments is essential.

**Structured Cabling:**

Employing a well-designed and organized cabling infrastructure is fundamental for a reliable Server Health Monitoring System. Structured cabling ensures that cables are properly labeled, organized, and managed, reducing the likelihood of cable-related issues that could impact connectivity.

**Power Redundancy:**

Power redundancy measures, such as uninterruptible power supply (UPS) systems, are crucial for server health monitoring. Power disruptions can lead to downtime and affect the availability of the monitoring system. Redundant power supplies and backup power sources mitigate this risk.

**Physical Cable Testing:**

Regularly testing and validating the physical cables used in the network infrastructure is essential. Faulty cables can introduce communication errors and negatively impact the performance of the Server Health Monitoring System. Cable testing tools can identify issues proactively.

**Temperature and Environmental Monitoring:**

Monitoring the physical environment in which servers and networking equipment are housed is vital. Elevated temperatures or humidity levels can affect the performance and reliability of hardware. Implementing environmental monitoring solutions helps identify and address issues related to the physical conditions of the server room or data center.

**Remote Management:**

Utilizing remote management capabilities for networking equipment and servers allows administrators to monitor and manage devices without physical access. This is particularly valuable for troubleshooting and performing maintenance tasks without the need for on-site presence.

**Physical Cable Management:**

Proper cable management practices, including cable trays, racks, and labels, contribute to the overall organization and tidiness of the server room or data center. Well-managed cables facilitate easier maintenance, troubleshooting, and scalability.

**Documentation and Labeling:**

Comprehensive documentation and labeling of physical network components, cables, and server configurations are essential for efficient management. Clear documentation helps in identifying and resolving issues quickly, reducing downtime during maintenance or troubleshooting activities.

By implementing these physical layer methodologies, organizations can establish a robust and reliable foundation for their Server Health Monitoring System, ensuring that the physical network infrastructure supports the continuous monitoring and management of server health.

**Subnetting :**

Subnetting plays a crucial role in any server health monitoring system by providing several key benefits:

**1. Improved Network Efficiency:**

* Subnetting divides a large network into smaller, more manageable subnets. This reduces the amount of broadcast traffic on the network, leading to improved performance and efficiency.

**2. Enhanced Security:**

* Subnets can be assigned different security policies and access controls, allowing administrators to segment sensitive servers and applications from the rest of the network.
* This can help to limit the impact of security breaches and improve overall network security.

**3. Simplified Network Management:**

* Subnetting makes it easier to manage and troubleshoot network problems.
* By isolating issues within specific subnets, administrators can quickly identify and resolve problems without impacting the entire network.

**4. Scalability:**

* Subnetting allows networks to be easily scaled to accommodate new servers and devices.
* This flexibility is critical for server health monitoring systems as the number of servers and monitored parameters often grow over time.

**5. Optimized Data Collection:**

* Subnetting can be used to optimize the location of monitoring agents and sensors.
* By placing agents and sensors within specific subnets, administrators can ensure efficient data collection and minimize network traffic overhead.

**6. Improved Monitoring Accuracy:**

* Subnetting can help to isolate and identify performance issues within specific server groups.
* This allows administrators to focus their attention on the most critical areas and take corrective action quickly.

**Implementation Strategies:**

There are several strategies for implementing subnetting in a server health monitoring system:

* Classless Inter-Domain Routing (CIDR): This is the most common method for subnetting. It allows for more flexibility and efficiency than traditional subnetting methods.
* Variable Length Subnet Masking (VLSM): This method allows for the creation of subnets with different sizes, depending on the specific needs of each server group.

## Hierarchical Subnetting: This method divides the network into multiple levels of subnets, providing a more granular level of control over network traffic. Virtual LAN (VLAN) in Server Health Monitoring System :

Virtual LANs (VLANs) can play a significant role in server health monitoring systems by providing several benefits:

**1. Network Segmentation:**

* VLANs divide a physical network into logical segments, isolating traffic and improving network performance. This is especially beneficial in large networks with diverse server groups.

**2. Security Enhancement:**

* VLANs can be used to implement different security policies for different server groups, restricting unauthorized access to sensitive servers and applications.
* This can help to prevent security breaches and data leaks.

**3. Improved Monitoring and Troubleshooting:**

* By isolating traffic within specific VLANs, administrators can more easily monitor and troubleshoot network issues.
* This can help to identify the root cause of problems more quickly and implement corrective actions efficiently.

**4. Traffic Optimization:**

* VLANs can be used to prioritize network traffic for critical servers, ensuring they receive the bandwidth and resources they need to perform optimally.
* This can improve overall server responsiveness and user experience.

**5. Scalability:**

* VLANs allow for flexible and scalable network expansion. New servers can be easily added to specific VLANs without affecting the rest of the network.
* This is important for server health monitoring systems that need to accommodate a growing number of monitored servers.

**Implementation Strategies:**

There are two main approaches to implementing VLANs:

* Port-based VLANs: This method assigns VLAN membership based on the physical port a device is connected to.
* 802.1x-based VLANs: This method assigns VLAN membership based on the user or device credentials.

802.1x-based VLANs typically offer greater security and control over port-based VLANs.

**Examples of VLAN Usage in Server Health Monitoring:**

* Production Servers: Servers running critical applications can be placed in separate VLANs with dedicated monitoring resources.
* Development Servers: Servers used for testing and development can be placed in separate VLANs to isolate traffic and prevent potential security breaches.
* Database Servers: Database servers can be placed in a dedicated VLAN with strict access controls to protect sensitive data.

**Results of a Server Health Monitoring System:**

* **Real-time Monitoring Data:**

Continuous data on server performance metrics such as CPU usage, memory usage, disk space, and network activity.

* **Alerts and Notifications:**

Immediate alerts or notifications triggered when predefined thresholds are breached, indicating potential issues with server health.

* **Historical Performance Trends:**

Historical data showing trends and patterns in server performance over time, aiding in proactive issue resolution and capacity planning.

* **Resource Utilization Metrics:**

Detailed insights into how server resources are utilized, helping administrators optimize resource allocation and prevent bottlenecks.

* **Uptime and Downtime Statistics:**

Records of server uptime and downtime, indicating the overall reliability and availability of the server infrastructure.

* **Security Incident Reports:**

Information on security-related events, anomalies, or potential breaches, allowing for swift response to safeguard server and network integrity.

* **Compliance Adherence:**

Reports on whether servers adhere to compliance standards and regulations, providing insights into the security and governance of the system.

**Inferences from a Server Health Monitoring System:**

* **Identifying Performance Issues:**

Analysis of real-time and historical data helps identify performance issues, allowing administrators to pinpoint and address root causes.

* **Proactive Issue Resolution:**

Early detection of anomalies and deviations from normal server behaviour enables proactive issue resolution, minimizing the impact on operations.

* **Optimizing Resource Allocation:**

Insights into resource utilization patterns assist in optimizing resource allocation, ensuring that servers operate efficiently without unnecessary strain.

* **Capacity Planning:**

Historical performance trends aid in capacity planning, helping organizations scale their server infrastructure in alignment with evolving business needs.

* **Enhanced Security Measures:**

Detection of security incidents and adherence to compliance standards contribute to the enhancement of security measures, reducing the risk of data breaches.

* **Improved User Experience:**

By ensuring server health and reliability, the Server Health Monitoring System contributes to an improved user experience by minimizing downtime and disruptions.

* **Data-Driven Decision Making:**

Administrators can make informed decisions based on the data provided by the monitoring system, guiding resource allocation, infrastructure upgrades, and strategic planning.

* **Cost Optimization:**

Efficient resource utilization and proactive issue resolution contribute to cost optimization by minimizing downtime-related financial losses and preventing unnecessary hardware upgrades.

* **Business Continuity:**

Ensures business continuity by identifying and addressing potential issues before they lead to critical failures, maintaining uninterrupted service for end-users.

* **Continuous Improvement:**

Regular analysis of monitoring data and inferences drawn from the system contribute to a continuous improvement cycle, where administrators can refine strategies and policies based on evolving server and network requirements.

In conclusion, a well-implemented Server Health Monitoring System provides valuable results and inferences that empower organizations to maintain a robust and reliable IT infrastructure, ensuring optimal server performance, security, and overall business continuity.

**Conclusion:**

In conclusion, a Server Health Monitoring System stands as a critical component in the management and optimization of IT infrastructure. Through continuous surveillance, analysis, and reporting of server performance, this system plays a pivotal role in ensuring the reliability, security, and efficiency of server operations. The following key points summarize the significance and benefits of a Server Health Monitoring System:

* **Enhanced server uptime and availability:** Proactive identification and resolution of potential issues minimize downtime and disruptions.
* **Improved server performance**: Bottleneck detection and resource optimization lead to faster response times and increased user satisfaction.
* **Reduced operating costs**: Automated monitoring and efficient resource allocation lower overall expenditure.
* **Enhanced security:** Continuous vigilance against suspicious activity and vulnerabilities mitigates cyber threats and protects sensitive data.
* **Data-driven decision making:** Accurate information facilitates informed choices regarding infrastructure investments and resource allocation.
* **Improved regulatory compliance**: Comprehensive monitoring and reporting capabilities simplify compliance with industry regulations.

In essence, a well-designed and effectively implemented Server Health Monitoring System serves as a cornerstone for maintaining a resilient, secure, and high-performing IT infrastructure. It empowers organizations to adapt to changing demands, mitigate risks, and deliver a seamless experience to end-users, ultimately contributing to the overall success of the business.

**Future Work for Server Health Monitoring Systems:**

While server health monitoring systems have made significant strides in recent years, there is still room for exciting developments and advancements. Here are some potential areas for future work:

**1. Artificial Intelligence (AI) and Machine Learning (ML):**

* **Predictive analytics:**Utilize AI and ML to predict potential server failures and performance issues before they occur, enabling proactive maintenance and preventing downtime.
* **Automated root cause analysis:** Employ AI algorithms to automatically identify the root cause of server problems, saving valuable time and resources for administrators.
* **Anomaly detection:**Develop AI-powered anomaly detection systems to identify unusual patterns and behaviour indicative of potential security threats or system instability.

**2. Cloud-based Monitoring:**

* **Leverage cloud platforms:** Develop server health monitoring systems that seamlessly integrate with cloud platforms, offering flexible deployment options and scalability.
* **Multi-cloud management:** Enable monitoring of servers across different cloud platforms, providing a unified view of server health across the entire IT infrastructure.
* **Edge computing integration**: Integrate server health monitoring with edge computing systems to gain insights into the performance and health of servers located at the edge of the network.

**3. Advanced Monitoring Techniques:**

* **Biometric authentication:** Implement biometric authentication for server access control, bolstering security and preventing unauthorized access.
* **Application performance monitoring (APM):** Integrate APM capabilities into the server health monitoring system to gain deeper insights into application performance and identify potential bottlenecks.
* **Network traffic analysis:** Analyse network traffic patterns to detect anomalies and identify security threats that may not be evident through traditional monitoring methods.

**4. Enhanced User Interface and Reporting:**

* **Intuitive dashboards:** Develop user-friendly dashboards that provide comprehensive visualizations of server health data in real-time.
* **Customizable reports:** Enable administrators to generate customized reports tailored to their specific needs and interests.
* **Automated alerting:** Implement automated alerting systems that notify administrators of critical issues and potential problems in a timely manner.

**5. Security and Privacy:**

* **Zero-trust security:** Implement zero-trust security principles to minimize the attack surface and ensure secure access to server health monitoring systems.
* **Data encryption:** Encrypt all sensitive data collected and stored by the system to protect against unauthorized access.
* **Privacy-preserving techniques:** Develop privacy-preserving techniques that allow for effective server health monitoring while minimizing the collection and storage of personal data.

By focusing on these areas of future work, server health monitoring systems can become even more intelligent, efficient, and valuable for organizations of all sizes. These advancements will further enhance server performance, improve security, and ultimately contribute to a more robust and resilient IT infrastructure

**Resources for Server Health Monitoring System with Links:**

**Open-source tools:**

* Prometheus: <https://stackoverflow.com/questions/53365191/monitor-custom-kubernetes-pod-metrics-using-prometheus>
* Grafana: <https://grafana.com/>
* Icinga: <https://icinga.com/docs/icinga-web/latest/doc/02-Installation/>
* Zabbix: <https://www.zabbix.com/>
* LibreNMS: <https://www.librenms.org/>

**Commercial tools:**

* SolarWinds Server & Application Monitor: <https://www.solarwinds.com/server-application-monitor>
* Dynatrace: <https://docs.dynatrace.com/docs/extend-dynatrace/opentelemetry/overview/traces>
* Splunk: <https://www.splunk.com/>
* Datadog: <https://www.datadoghq.com/>
* AppDynamics: <https://www.appdynamics.com/>

**Articles and tutorials:**

* Server Monitoring Best Practices: 9 Tips to Improve Health and Performance: <https://sematext.com/server-monitoring/>
* Server Health Monitoring | Introduction & Tools: 2023: <https://sematext.com/blog/server-monitoring-tools/>
* 10 Best Server Monitoring Tools & Software [2023 Review]: <https://sematext.com/server-monitoring/>

**Books:**

* Monitoring and Managing Your Servers with Nagios: <https://www.amazon.com/Nagios-Network-Monitoring-Wolfgang-Barth/dp/1593271794>
* The Art of Monitoring: Building a Robust and Scalable Monitoring System: <https://www.amazon.com/James-Turnbull/e/B002BLLCPI>
* Site Reliability Engineering: <https://books.google.com/books?id=_4rPCwAAQBAJ&printsec=frontcover>

**Additional resources:**

* Linux Foundation Training: Certified System Administrator (LFS151): <https://www.edx.org/school/linuxfoundationx>
* Cloud Academy: Server Monitoring and Management: <https://cloudacademy.com/course/introduction-to-operations/monitoring-2/>
* Coursera: Monitoring and Managing Cloud Resources with Azure Monitor: <https://learn.microsoft.com/en-us/training/modules/intro-to-azure-monitor/>

**References for Server Health Monitoring System:**

**Articles:**

* Server Monitoring Best Practices: 9 Tips to Improve Health and Performance: <https://www.comparitech.com/net-admin/server-monitoring-best-practices/>
* Server Health Monitoring | Introduction & Tools: 2023: <https://www.servertribe.com/server-health-monitoring/>
* 10 Best Server Monitoring Tools & Software [2023 Review]: <https://sematext.com/server-monitoring/>
* What Is Server Health Monitoring? <https://www.extnoc.com/>
* Server Health Monitoring and Reporting: <https://www.solarwinds.com/server-application-monitor/use-cases/server-health-monitoring>

**Books:**

* Monitoring and Managing Your Servers with Nagios: by Wolfgang Barth, Peter Hanebuth (2007)
* The Art of Monitoring: Building a Robust and Scalable Monitoring System: by James Turnbull (2014)
* Site Reliability Engineering: by Betsy Beyer, Chris Jones, Jennifer Petoff, Niall Richard Murphy (2016)

**Websites:**

* Prometheus: <https://prometheus.io/>
* Grafana: <https://grafana.com/>
* Icinga: <https://icinga.com/>
* Zabbix: <https://www.zabbix.com/>
* LibreNMS: <https://www.librenms.org/>
* SolarWinds Server & Application Monitor: <https://www.solarwinds.com/server-application-monitor>
* Dynatrace: <https://docs.dynatrace.com/docs/extend-dynatrace/opentelemetry/overview/traces>
* Splunk: <https://www.splunk.com/>
* Datadog: <https://www.datadoghq.com/>
* AppDynamics: <https://www.appdynamics.com/>
* Linux Foundation Training: Certified System Administrator (LFS151): <https://www.edx.org/learn/linux/the-linux-foundation-introduction-to-linux>
* Cloud Academy: Server Monitoring and Management: <https://cloudacademy.com/>
* Coursera: Monitoring and Managing Cloud Resources with Azure Monitor: <https://learn.microsoft.com/en-us/training/modules/azure-monitor/>

**Other Resources:**

* System Design — A Server Health Monitoring System: <https://medium.com/@ajingnv/system-design-a-server-health-monitoring-system-9bdd0066bb9c>
* Physical Layer Methodologies for Server Health Monitoring System: <https://www.wired.com/story/google-bard-location-data-tracking-ai/>
* Subnetting in Server Health Monitoring System: <https://timesofindia.indiatimes.com/gadgets-news/who-has-a-health-warning-on-chatgpt-and-google-bard/articleshow/100291641.cms>
* Virtual LAN (VLAN) in Server Health Monitoring System: <https://www.theguardian.com/technology/2023/feb/09/google-ai-chatbot-bard-error-sends-shares-plummeting-in-battle-with-microsoft>