Network monitoring

Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages or other trouble. Network monitoring is part of network management.[1]

Contents

Details

While an intrusion detection system monitors a network threats from the outside, a network monitoring system monitors the network for problems caused by overloaded or crashed servers, network connections or other devices.

For example, to determine the status of a web server, monitoring software may periodically send an HTTP request to fetch a page. For email servers, a test message might be sent through SMTP and retrieved by IMAP or POP3.

Commonly measured metrics are response time, availability and uptime, although both consistency and reliability metrics are starting to gain popularity. The widespread addition of WAN optimization devices is having an adverse effect on most network monitoring tools, especially when it comes to measuring accurate end-to-end delay because they limit round-trip delay time visibility.[2]

Status request failures, such as when a connection cannot be established, it times-out, or the document or message cannot be retrieved, usually produce an action from the monitoring system. These actions vary; An alarm may be sent (via SMS, email, etc.) to the resident sysadmin, automatic failover systems may be activated to remove the troubled server from duty until it can be repaired, etc.

Monitoring the performance of a network uplink is also known as network traffic measurement.

Network tomography

Network tomography is an important area of network measurement, which deals with monitoring the health of various links in a network using end-to-end probes sent by agents located at vantage points in the network/Internet.

Route analytics

Route analytics is another important area of network measurement. It includes the methods, systems, algorithms and tools to monitor the routing posture of networks. Incorrect routing or routing issues cause undesirable performance degradation or downtime.

Various types of protocols

Site monitoring services can check HTTP pages, HTTPS, SNMP, FTP, SMTP, POP3, IMAP, DNS, SSH, TELNET, SSL, TCP, ICMP, SIP, UDP, Media Streaming and a range of other ports with a variety of check intervals ranging from every four hours to every one minute. Typically, most network monitoring services test your server anywhere between once-per-hour to once-per-minute.

For monitoring network performance, most tools use protocols like SNMP, NetFlow, Packet Sniffing, or WMI.

Internet server monitoring

Monitoring an internet server means that the server owner always knows if one or all of his services go down. Server monitoring may be **internal**, i.e. web server software checks its status and notifies the owner if some services go down, and **external**, i.e. some web server monitoring companies check the services status with a certain frequency. Server monitoring can encompass a check of system metrics, such as CPU usage, memory usage, network performance and disk space. It can also include application monitoring, such as checking the processes of programs such as Apache HTTP server, MySQL, Nginx, Postgres and others.

External monitoring is more reliable, as it keeps on working when the server completely goes down. Good server monitoring tools also have performance benchmarking, alerting capabilities and the ability to link certain thresholds with automated server jobs, such as provisioning more memory or performing a backup.

Servers around the globe

Network monitoring services usually have a number of servers around the globe - for example in America, Europe, Asia, Australia and other locations. By having multiple servers in different geographic locations, a monitoring service can determine if a Web server is available across different networks worldwide. The more the locations used, the more complete is the picture on network availability.

Web server monitoring process

When monitoring a web server for potential problems, an external web monitoring service checks a number of parameters. First of all, it monitors for a proper HTTP return code. By HTTP specifications RFC 2616, any web server returns several HTTP codes. Analysis of the HTTP codes is the fastest way to determine the current status of the monitored web server. Third-party application performance monitoring tools provide additional web server monitoring, alerting and reporting capabilities.

Notification

As the information brought by web server monitoring services is in most cases urgent and may be of crucial importance, various notification methods may be used: e-mail, land-line and cell phones, messengers, SMS, fax, pagers, etc.

See also

- Business service management
- Comparison of network monitoring systems
- High availability
- Network Monitoring Interface Card
- Network traffic measurement
- Network tap
- System monitor
- Service-level agreement

Notes and references

1. Ratan, Vivek; Li, Kin Fun (2016-10-22), "NetFlow: Network Monitoring and Intelligence Gathering" (https://dx.doi.org/10.1007/978-3-319-49109-7_83), *Advances on P2P, Parallel, Grid, Cloud and Internet Computing*, Cham: Springer International Publishing, pp. 863–867, ISBN 978-3-319-49108-0, retrieved 2020-11-01
2. "The impact of WAN Optimization on NetFlow/IPFIX measurements" (https://web.archive.org/web/20111224180921/http://www.networkperformancedaily.com/2007/07/whiteboard_series_the_impact_o_1.html). Archived from the original (http://www.networkperformancedaily.com/2007/07/whiteboard_series_the_impact_o_1.html) on 2011-12-24. Retrieved 2007-07-19.

External links

- Network Management (https://curlie.org/Computers/Software/Networking/Network_Management) at Curlie
- List of Network Monitoring and Management Tools at Stanford University (http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html)