Monitoring the IT infrastructure in a technical enterprise and its importance

Goldberger Christian, k01555869

PS Communication Engineering, SE Fachsprache Englisch

*Abstract*— The increasing number of devices in a company makes it more difficult to keep track of them. It can often lead to serious consequences, if a device fails. Thus, a functioning IT infrastructure is indispensable for the continuation of a company. To keep an eye on the availability of the devices, it is recommended to use a monitoring system., but the variety of monitoring systems on the market often make it difficult to choose the right solution. In this paper, we will discuss the term monitoring and IT monitoring. Furthermore, we will discuss different types of monitoring and protocols. In addition, we will discuss various criteria that should be considered when choosing a monitoring tool. Finally, we will compare two concrete monitoring tools against these criteria.

Keywords—monitoring; infrastructure; protocols; network; selection criteria

# Introduction

Nowadays, a smoothly functioning IT infrastructure is indispensable in a company. Modern IT infrastructures are becoming increasingly networked and are scaling strongly. As a result, the number of devices and technologies in the enterprise continues to grow, and the associated configuration and maintenance effort also increases. To ensure a smooth business process, the entire IT infrastructure must function flawlessly. Disruptions and failures in the operational procedures are quickly reflected in time and especially financial losses. To keep an eye on availability, performance and bandwidth utilization in an IT network, the use of a monitoring system can be beneficial. However, every organization has different requirements for a monitoring solution, and as the market now offers many various tools and solutions, it is therefore difficult to decide on a suitable system. [1] [2] [3] [4]

During an internship as an IT administrator where, the main focus was on monitoring, there was a particular problem that stood out to me. The problem was that monitoring an IT infrastructure was difficult due to the lack of a monitoring system. It was hard to get an overview of which devices were active in the company or not. Therefore, this paper’s aim is to show the basic terms of monitoring systems and underlining the importance of monitoring systems and to give some suggestions on what should be taken into consideration when choosing a monitoring system.

Thus, this paper shows what can be understood by monitoring and what opportunities a monitoring system can offer. It also gives an overview of the most common monitoring types and protocols and the classification of monitoring systems. Furthermore, this paper is intended to help selection criteria, to help with the decision-making process of a system, and it compares two specific network monitoring systems that would be suitable for monitoring purposes.

To answer all these areas, we start with the general term monitoring and what you can understand by IT monitoring. After the definition of the term, we look at the most common monitoring types and protocols. After that we emphasize, how network monitoring systems can be classified and what endless possibilities a network monitoring system can offer. Below, I will also mention helpful selection criteria that can help with the selection of a network monitoring system. Finally, I will compare two monitoring systems based on their advantages and disadvantages.

# Monitoring

Monitoring is an umbrella term for all types of direct systematic acquisition, measurement, observation or monitoring of an operation or process by means of technical aids or other observation systems. Repeated regular performance is a central element of the respective research programs in order to draw conclusions from results comparisons. [1] [2] [3] [4]

## A. IT Monitoring

Monitoring in the field of IT means monitoring or ongoing control for proper functionality. It is a term that describes the logging and detection of processes. Monitoring is one of the most important tasks for a system administrator. It can monitor all major computers, computer systems and networks, both hardware and software. Such a system is characterized by low system load, although it counts the individual measuring points continuously and thoroughly around the clock. [1] [2] [3] [4]

It can notify the employee concerned at an early stage of the error. Various access systems and remote maintenance concepts enable the status of the IT infrastructure to be viewed anytime, anywhere. The clear advantages of a monitoring system are the increase in availability, as well as the stability, 24/7 monitoring, early detection and notification in case of error, automatic visualization and evaluation. [1] [2] [3] [4]

## B. Active Monitoring

During active monitoring, active test clients are installed in the network. Active connections to the test clients are established from a central monitoring station and data / packets are transmitted on an ongoing basis. This makes it possible to better monitor end-to-end connections (VoIP). Signal changes can be better detected during active monitoring. Disadvantage is the increased parcel shipping in the net for monitoring purposes. [3] [4]

## C. Passive Monitoring

In this case no additional packets are sent in the network, but the data traffic is simply overheard at certain nodes. These data streams are mirrored to the monitoring system and then the data is analyzed. The clear advantage is that no additional network loads are caused. [3] [4]

## D. Monitoring Types and Protocolls

To monitor the various hardware and software, there are several ways in which the data can be tapped. This can be done via standardized protocols or by manufacturer-specific services. Regarding this, the basic terms and functions of the most common types of monitoring are briefly clarified.

### Simple Network Monitoring Protocoll (SNMP)

SNMP is used to monitor and configure network devices. It must be activated on the device to be monitored and is then addressed via the network. The protocol is very simple and causes very little traffic. It is also suitable for low power devices (e.g., temperature sensors). The device sends information on request from a management console over the network. It is also possible to send automated messages, so-called traps, in the event of a fault or status change and to evaluate them. For this purpose, a request is sent to the device to be monitored, which responds with a response or a trap. [1] [2] [3] [4] [5]

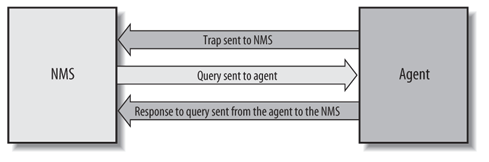


Figure 1: Relationship between an NMS and an agent [8]

The SNMP agent is the network device that is addressed by the central management console It must be activated accordingly before use. [3] [5] [6]

The SNMP client is the actual management console and is the link between man and machine. It manages the SNMP agents and reads the received data. The client thus represents the actual IT monitoring system. [3] [5] [6]

### Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is part of the Internet Protocol (IP), but is handled independently. It is used to transmit messages via IP, more precisely, status information and error messages of the IP, TCP and UDP protocols are to be transmitted. [5] [6] [8] [9]

The most popular tools that fall under ICMP are "Ping" and "Trace Route". The feedbacks triggered by these commands can be analyzed with a network monitor.

Ping is the most widely used tool to test a network connection.

[5][6] [8] [9]

In this case, ICMP packets of the Echo Request type are sent to the remote device, which sends back an ICMP packet of the Echo Reply type on availability. If the terminal is not available, you will get an error message back. Thus, the availability of various devices in the network can be checked very easily using ICMP Ping. [5] [6] [8] [9]

### Simple Objectiv Access Protocol (SOAP)

SOAP is a network protocol that allows data to be exchanged between systems. It is an industry standard of the W3C. It relies on XML for data representation and transport and application layer Internet protocols for messaging (HTTP, TCP). The XML message design is exactly regulated in SOAP, as is the interpretation of the data. [10]

This protocol is used for remote procedure calls, message systems or data exchange. In practice, data is usually sent via HTTP. SOAP is also used when exchanging between very different systems where there might be compatibility issues. A SOAP message consists of an envelope element, this usually contains a header part with meta-information and a body part, in which the actual user data are stored. [10]

### Network Sniffer

A network sniffer monitors the data flow in the network in real time. Sniffers can be built both as hardware and software. All network packets of a certain interface are monitored and copied and can then be evaluated and filtered. In addition to individual data packets, the content of these can be analyzed very precisely (destination addresses, source addresses, etc.). [11]

By default, the network card of the computer on which the sniffer is running, but also forwarding other interfaces to a central point (port mirroring) is possible. The load in the network is significantly higher when sniffing than with other methods and is not realized in practice over longer periods of time. The classic application can be found in the error analysis, in a short period of time mostly over a few hours or days. [11]

### Netflow

Netflow is a network protocol designed to collect and monitor information about network traffic. Using a NetFlow-Collector and -Analyzer, the incoming and outgoing network data of a network device can be evaluated.

The data is exported via the IP data stream from the switch or router via UDP (Netflow Exporter). These datagrams are collected, stored and processed by a management system (Netflow Collector). [12]

Netflow is a passive measurement method that means you do not affect the traffic. UDP transmission does not affect the performance of the network, but lost data packets can no longer be produced. This is often problematic especially for flows over an internet connection. [12]

To summarize, monitoring itself is an umbrella term for all types of recording, measuring, observation or monitoring of operations. There are many different types of monitoring. IT monitoring deals with the monitoring of computers, computer systems as well as networks of the entire IT infrastructure in a company. In monitoring, two types of active and passive monitoring are distinguished. With active monitoring, concrete test clients are installed in the network. Whereas, with passive monitoring, only the data traffic is overheard, and this data is sent to the monitoring system and subsequently get evaluated. Furthermore, there are different types and protocols for monitoring. On the one hand, the Simple Network Monitoring Protocol (SNMP) is applied. This is used to monitor and configure network systems. The Internet Control Message Protocol (ICMP) is part of the Internet Protocol (IP) and is used to send messages more precisely over IP. Another protocol is Simple Objective Access Protocol (SOAP), which is used to send data between different systems. To monitor the data flow in a network, a so-called network sniffer is applied and the Netflow is a protocol designed to monitor and collect information of the network traffic.

# How to Select a tool

The right choice for a monitoring system is usually not easy. The large number of manufacturers offers you many monitoring systems. Finding the right tool for the right application is usually a big challenge. So, the following points should clarify what you should consider when choosing a monitoring system.

## Costs

A key point in finding a suitable software is the funding of this. We differentiate between the acquisition costs, which are due at the beginning of the implementation and the running costs (usually known in the IT sector as maintenance costs), which recur periodically and usually give access to new versions or bug fixes as well as the manufacturer's support. Usually a budget is prescribed by the management for a project, which may not be exceeded. [13] [14] [15]

## Initial Configuration

For the initial configuration, the executive employee must spend more or less working time. Since this time is often more expensive for the company than the cost of the software itself. Depending on the complexity and ease of use, the initial configuration can take anywhere from a few hours or days to several weeks. In some cases, you also need external know-how, which can also lead to high costs. [13] [14] [15]

## Maintenance

After initial configuration, the system should run satisfactorily. In practice, however, shows that changes, adjustments and extensions are necessary again and again. These activities fall under the term maintenance or maintenance requirements. It depends mainly on the usability of the system, how much effort we must invest to be able to handle the desired new requirements. [13] [14] [15]

## Surveillance methods

Each monitoring software usually has a specialization. If you want to monitor all IT systems in a company, you need a broad portfolio of monitoring methods. However, if only one specialty has to be mapped, specializing in these monitoring protocols is a good idea. If, for example, only network traffic needs to be monitored, a special software that deals with Netflow is enough. [13] [14] [15]

## Cloud connectivity

Cloud connectivity is indispensable in today's everyday life. Therefore, the possibility of using cloud services must be considered. Which services can be used and how? For example, a notification or an alarm can be sent by means of cloud services, or data storage and data access can take place via such systems. It is important to estimate the meaning, since cloud services are usually associated with costs. [13] [14] [15]

## Mobility

Mobility is another core topic which should be considered. There are many ways to make a tool accessible online. One of the decision criteria is the availability on different platforms such as Android or iOS, or the classic availability via a web browser. We also should consider what information we can provide here. Often this is not intended by the manufacturer. Eventually, access via a secure connection (e.g., VPN) is also a possible way to ensure mobility. [13] [14] [15]

## Variation in Alerting

How can mistakes be brought to the employees? There are different approaches and implementation variants from the manufacturers. Redundancy is paramount here. Should an alerting variant fail, the information must still be able to reach the employee in the event of an error. Often the systems provide ready-made mail delivery options, sometimes you can also connect your own servers. [13] [14] [15]

## Across Locations

Due to growing infrastructures and several company locations, there cannot always be a direct network connection through the system. The monitoring tool must offer an easy way to monitor external locations or possibly isolated systems at customers or suppliers and to provide the employees concerned with information about these devices at any time. The best without having to set up a VPN tunnel or similar access concepts. [13] [14] [15]

## Usability

The configuration is usually only the beginning for the introduction of an overall system. Once the system is running, it must also be easy to use. The operability must also be possible for employees without background knowledge of the system. This is about data view and data evaluation and not about configuration work. Thus, a clear user interface, a certain adaptability, and a quick orientation in the application, are important criteria in the selection of a suitable software solution. A complicated operation often leads to failure, at the latest when switching to continuous operation, even if the actual functionality of the software otherwise would be ideally suited. [13] [14] [15]

## Security

A security concept for IT systems is nowadays indispensable. Starting with access management, through permissions to encrypted transmission, the topic of security in IT is very important. Since a monitoring tool is used to access a wide range of core systems from different departments and their employees, there must be certain restrictions here. Thus, a user or group administration, as well as the adjustment of the access rights is a core issue for the security concept. In addition, data backup via an existing backup system of the company is an important security criterion. [13] [14] [15]

To summarize again, the right choice for a monitoring system can be very difficult due to the large number of such systems. Before deciding which system is the right one, you should consider several points. For example, costs are a big factor, because we have to pay attention to maintenance costs in addition to the acquisition costs. As well as initial configuration, system maintenance should also be considered, as these points are often associated with a lot of effort. Furthermore, we should consider which monitoring methods we want to use and whether the system has a cloud connection and mobility. In addition, we should think about how we want to be alerted in the case of an error and whether the system can eliminate these errors automatically. Since larger companies also have several locations, we should also consider whether the system is across locations. However, these points should also be consistent with the usability, as people without background knowledge should be able to use this system. Last but not least, security should not be ignored, since the company usually deals with sensitive data.

# Whats up Gold and PRTG

In this point, two concrete monitoring systems are compared against the criteria which have been discussed in the previous point.

## WHATS UP GOLD

WhatsUp Gold is developed by Ipswitch and is one potential software solution that can monitor enterprise infrastructure performance, configuration and connectivity across wired, wireless, physical and virtual devices. The following table shows what qualifications WhatsUp Gold offers regarding to the criteria for selecting a monitoring tool.

|  |  |
| --- | --- |
| Costs | 1400€/one-time, extra costs for each device |
| Initial Configuration | Access via web interface; network scan to identify device addresses; auto generated map of all devices |
| Maintenance | Very easy; network scan adds devices to server; updates can be rolled out via program |
| Surveillance methods | All common surveillance methods, eg. SNMP-Monitoring, Netflow, etc. |
| Cloud connectivity | Easy access to cloud services (e.g. Amazon Cloud, Microsoft Azure) |
| Mobility | No app for smartphones; access to server via VPN |
| Variation in Alerting | Mail, messages, acoustic alerting |
| Across Locations | No across locations functionality available; VPN is necessary |
| Usability | User interface can sometimes be very confusing |
| Security | User principles can be added |

Table 1: Whats Up Gold compared to the selection criteria

## PRTG

PRTG is another infrastructure monitoring solution. It was developed by the manufacturer Paessler and monitors the individual devices with so-called sensors. The following table shows as well what qualifications PRTG offers regarding to the criteria for selecting a monitoring tool.

|  |  |
| --- | --- |
| Costs | 500 sensors cost around 400€, incl. 12-month maintenance |
| Initial Configuration | Network scan to identify all devices and their sensors; Possibility to create groups for devices; manual addition of devices available |
| Maintenance | Very easy; Group principles for devices |
| Surveillance methods | All common surveillance methods, eg. SNMP- Netflow, FTP, HTTP etc. |
| Cloud connectivity | Access to all common cloud services (e.g. Amazon Cloud) |
| Mobility | Web access and app for Android and IOS |
| Variation in Alerting | Mails, messages, SNMP, push-messages |
| Across Locations | Access via VPN and remote via web interface |
| Usability | Easy and intuitive |
| Security | User principles can be added |

Table 2: PRTG compared to the selection criteria

As we can see from the tables, the two systems differ only slightly from each other. So, you have to pay for WhatsUp Gold 1400 € one-time and you also have to pay some extra costs for each device. With PRTG, on the other hand, you have to pay for a certain number of sensors. Both systems also differ in terms of mobility and access to different locations. WhatsUp-Gold does not offer an app and can only be accessed across locations via VPN. In contrast, PRTG offers an app for Android and IOS as well and access to various locations via a web interface.

# Conclusion

In this paper we discussed the monitoring of the infrastructure in a technical company and its importance. We started with the term monitoring and IT monitoring and looked at the different types of monitoring and protocols. Furthermore, we looked at the criteria for the right choice of a monitoring tool and we compared two specific monitoring systems based on these selection criteria.

In conclusion, a monitoring tool offers clear advantages to keep track of the large number of devices. However, it is often very difficult to choose the right monitoring solution, because of the huge variety of monitoring systems on the market. The discussed selection criteria should help by choosing the right monitoring tool and they can be extended at any time.

##### References

1. ARPÈGE Group, Hrsg., Network Management. Dordrecht: Springer Netherlands, 1994.
2. H. Schubert, Hrsg., Netzwerkmanagement: Koordination von professionellen Vernetzungen: Grundlagen und Praxisbeispiele, 1. Auflage. Wiesbaden: VS Verlag für Sozialwissenschaften, 2008.
3. S. B. Moon, R. Teixeira, S. Uhlig, und PAM, Hrsg., Passive and active network measurement: 10th international conference, PAM 2009, Seoul, Korea, April 1-3, 2009 ; proceedings. Berlin: Springer, 2009.
4. M. Zitterbart und Gesellschaft für Informatik, Hrsg., Kommunikation in verteilten Systemen. Berlin: Springer, 1997.
5. T. Schwenkler, Sicheres Netzwerkmanagement: Konzepte, Protokolle, Tools. Berlin ; New York: Springer, 2006.
6. B.-Y. Choi, Z.-L. Zhang, und D. H.-C. Du, *Scalable Network Monitoring in High Speed Networks*. New York, NY: Springer New York, 2011.
7. K. Garbe, *Management von Rechnernetzen*. Wiesbaden: Vieweg+Teubner Verlag, 1991.
8. K. Schmidt and D. Mauro: Essential SNMP. Gravenstein Highway Noth, Sebastopol, O’Reilly Media, 2005
9. David J. Marchette -Computer Intrusion Detection and Network Monitoring\_ A Statistical Viewpoint-Springer-Verlag New York (2001).
10. D. Box u. a., Simple object access protocol (SOAP) 1.1. 2000.
11. Roger A. Grimes (auth.)-Honeypots for Windows-Apress (2005).
12. Y. Xiang, M. Pathan, X. Tao, und H. Wang, Hrsg., Internet and Distributed Computing Systems, Bd. 7646. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.
13. K. Fatema, V. C. Emeakaroha, P. D. Healy, J. P. Morrison, und T. Lynn, „A survey of Cloud monitoring tools: Taxonomy, capabilities and objectives“, J. Parallel Distrib. Comput., Bd. 74, Nr. 10, S. 2918–2933, Okt. 2014.
14. Ł. Kufel, „Tools for Distributed Systems Monitoring“, Found. Comput. Decis. Sci., Bd. 41, Nr. 4, Jan. 2016.
15. J. Hernantes, G. Gallardo, und N. Serrano, „IT infrastructure-monitoring tools“, IEEE Softw., Bd. 32, Nr. 4, S. 88–93, 2015.