Continuous Monitoring

Measuring is knowing when you know what you are measuring by applying Continuous Monitoring.

By Bart de Best

Context:

This practical example comes from a government organization that wanted to gain control over the service provision of tens of thousands of users working in hundreds of locations.

Challenge:

The service provided included 150 administrators, 40 separate monitoring tools and hundreds of infrastructure components. The SLA standards could only be measured at product level, but not at service level. Performance drops were almost impossible to pinpoint. There was a feeling of not being in control with high costs in terms of lost hours.

Solution:

The solution to this challenge has been found in the concept of Continuous Monitoring. This blog discusses this approach through the following steps:

1. Monitor architecture definition
2. Service definition
3. Building block plate
4. Monitor classification model
5. Monitor matrix model
6. SLA reporting

1. Monitor architecture definition

Figure 1 shows the current situation. This shows that the various components are collected by operators and passed on to the service desk. A service report is created based on defined service standards.

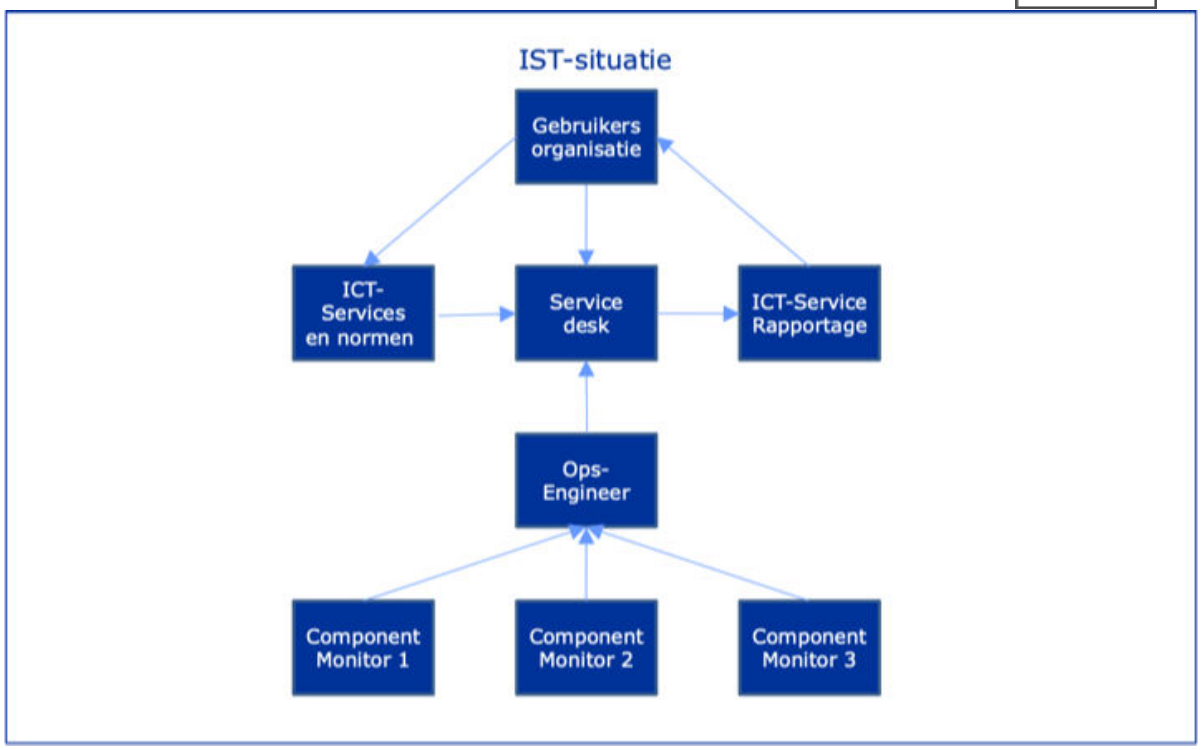


Figure 1, The current situation of the monitor facility.

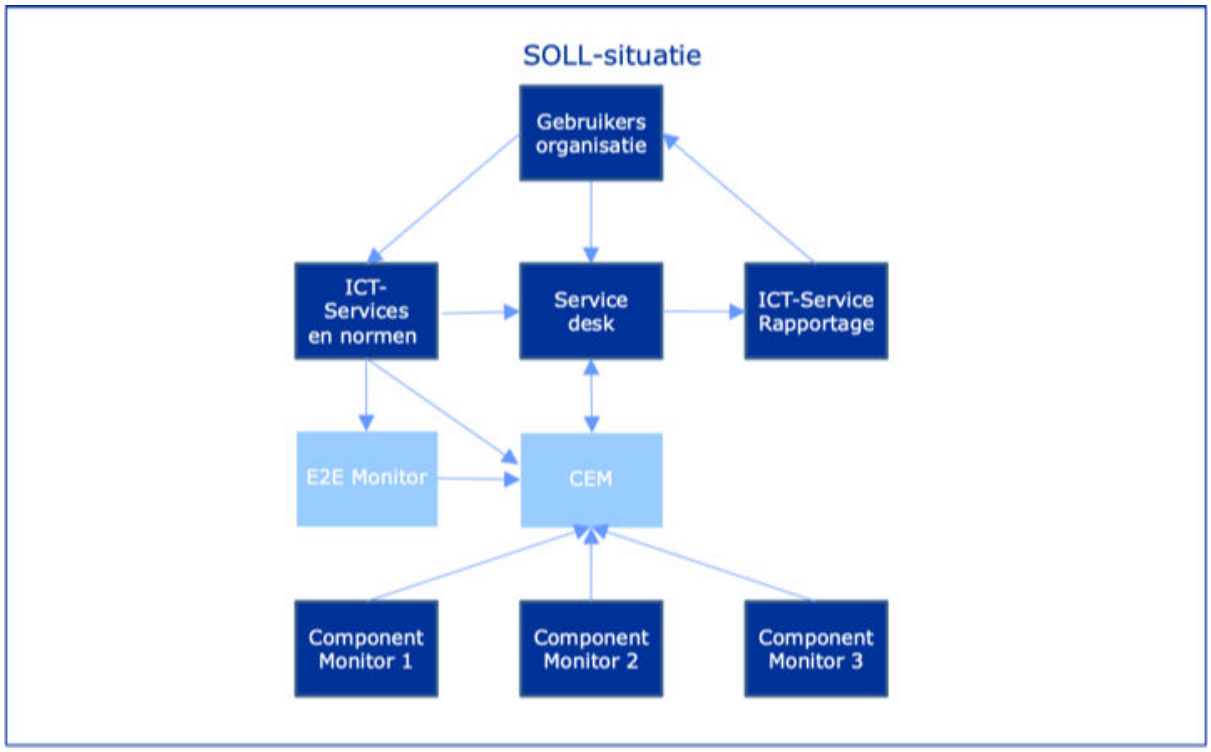


Figure 2, The desired situation of the monitor facility.

Figure 2 shows what the desired change includes.
This shows the End-to-End monitoring (E2E monitoring) that measures the entire chain of components from a user perspective. The Central Event Management (CEM) is also shown, which takes care of the automatic collection of events from

components and compares them with the E2E measurements. Incidents are automatically created by the CEM in the service desk based on set SLA standards.

2. Service definition

The Architecture Models are translated into a service design by mapping the application and infrastructure components for the service to be monitored. It has been determined which component monitoring tools are available for the application and infrastructure components. It has also been determined which monitor information is available.

3. Application and infrastructure building blocks plates

The service included one central application and many infrastructural facilities such as a WAN, LAN, Internet connection, mainframe, mini, database, etc. A building block plate has been drawn up for the application, divided into layers. This has also been done for the infrastructure provision.

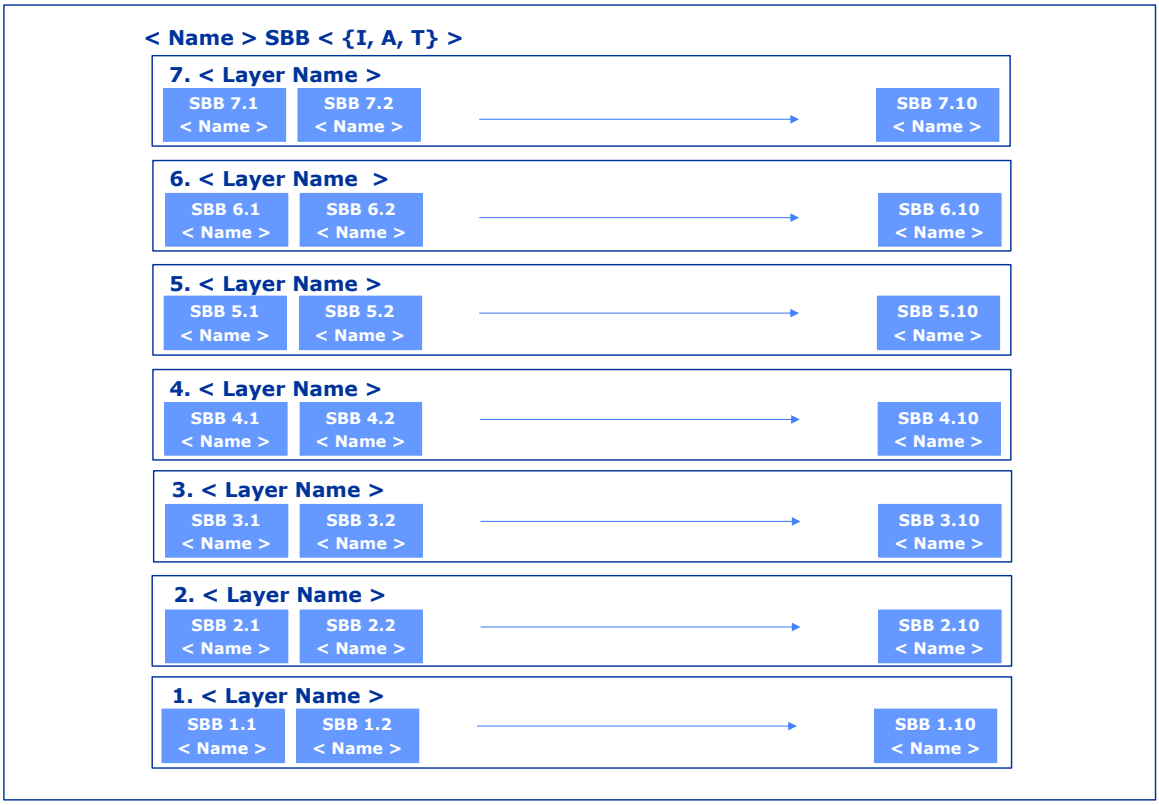


Figure 3. Building block plate template.

4. Monitor classification model

Based on this functional decomposition, it was determined for each building block which monitor facility could best be applied. The simplified monitor layer model was used for this purpose as shown in Figure 4.

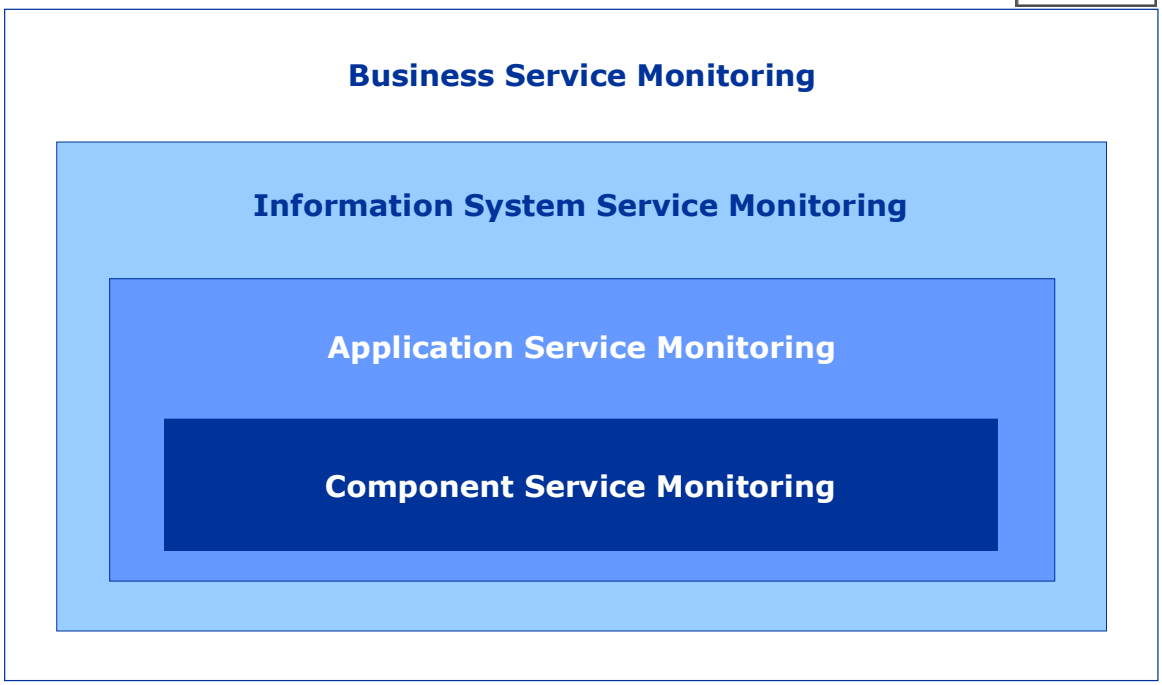


Figure 4. Simplified monitor layer model.

End User Experience monitoring

An End User Experience (EUX) facility was chosen for E2E monitoring. This is located at the application service monitoring layer because only one application is measured and not a number as with information system service monitoring. The EUX monitoring involves a robot that periodically imitates a user from any geographical location. The measurements were used to monitor the SLA and report the SLA standards.

End-to-End ping monitoring

In addition to the EUX monitoring, the designers of the monitor facility have also built a so-called E2E ping monitor. This is an infrastructure-level measurement that tracks the path of the network traffic that the application uses. The measurement is performed by building a dummy logic on each component that receives and forwards a message with date and time. This was designed and built in two days and offers the possibility to measure the lead time of the EUX monitoring of the application and that of E2E separated from the infrastructure traffic. In the event of a performance problem, it can immediately be seen whether it is application or infrastructural in nature.

For Central Event Monitoring, the existing CEM has been expanded with links to the required service monitoring component. This allows all 40 separate component monitoring tools to transmit the events to the CEM, which compares them with the EUX monitoring and the E2E ping monitoring.

5. Monitor matrix model

Figure 5 shows the monitor matrix model. This matrix is used to periodically detect deviations in the monitoring facility. If both E2E and component measurements have the same colour (green or red) then it is a good measurement. But if these contradict each other, an adjustment must be made to the monitor facility.

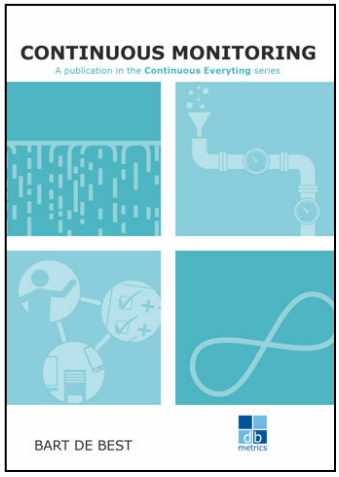
Monitor Verification Matrix		Component-based measurements	
		Within norms	Outside norms
E2E-measurements	Within norms	Service norms have been met.	Determine whether and how the E2E monitor functionality needs to be adjusted.
	Outside norms	Determine if and how the component-based monitor functionality can be customized.	Determine which infrastructure or application deficiencies are underlying these disruptions.

Figuur 5, Monitor matrix model.

6. SLA reporting

This form of monitoring makes it possible to continuously monitor the service. It also gives an impression of the service provided from the user's perspective. The SLA is sometimes also called an XLA. This monitoring also shows where a disruption is located (localization). Finally, a trend analysis of the performance is possible, and the cause of the performance degradation can be determined quickly and accurately. The monitor facility can be used in any environment. For example, developers can test the monitoring facility at an early stage to signal events from new or modified components.

By Bart de Best
DutchNordic.Group



https://www.dbmetrics.nl/ce-en/continuous-monitoring-en/