

# 1 TYPO3-Website-Monitoring

A Website is a complex mix of hardware, operating system and applications. In case of complex extendable solutions like TYPO3 also the installed extensions have to be monitored. Because of that it is difficult to completely monitor such a system especially when new security concerns arise or different systems, extensions or partners are interacting. Currently available system-monitoring software, like nagios, can check the hardware state and much more but not the proper setup of TYPO3 and the correct function of the whole website.

Authors:

- Thomas Hempel [n@work](#) Hamburg
- Martin Ficzel, [n@work](#) Hamburg
- Christoper Hlubek, networkteam Kiel/Hamburg
- Tobias Liebig, networkteam Kiel/Hamburg

For professional webhosting a continuously and complete monitoring of the it-infrastructure is needed. In complex system setups like TYPO3-Installation which consist of many interdependent parts this is getting very complicated. Usually software like nagios is used to monitor hard- and software. But often the monitored services depend more on the abilities of the monitoring software than on the needs of the website.

Usually a central monitoring server is communicating with sensors on the monitored system. This way the current state of the hardware and informations about running processes and pending security updates can be checked. Additionally ping and http requests are sent to the target machine and the response is checked.

**Making the decision which services are monitored by just taking the features of the monitoring software is dangerous because you can easily overlook some business critical aspects. We recommend to start with analyzing the critical services of the website and afterwards define the needs for the monitoring software.**

The following articles line out some general aspects for those decisions:

### 1.1 Availability: Is everything working?

The base oft availability monitoring is always the monitoring of the infrastructure, wich means hard- and software of the webserver. The network infrastructure and DNS must be included to. Additionally we recommend automated integration tests for business critical services. Therefore a browser session is recorded and replayed automatically. Like in Unit testing you have to be careful not to tests too many aspects in a single tests to get meaningful errors if problems occur.

### 1.2 Security: Is my website save?

The monitoring of system security usually checks for security-updates on os-level. But also the running application must be included, especially if it can be extended like TYPO3. So the security monitoring has to include not only the security of the core-application but also of extensions and the whole configuration. To perform this task insider knowledge regarding the specific application is needed.

### 1.3 Performance: Are there any bottlenecks?

Performance monitoring is done by continously recording some performance indicators to detect changes for beeing able to react in time. More important than a single value is the chronological development. A graphical representation of the recorded data is necessary for interpretation.

Those 3 aspects are highly dynamic on big websites so a simple and flexible management of the monitoring is another prerequisite. Additionally a hierarchical structure is needed to remain focused even in complex scenarios with many websites and hundreds of tests. The existing solutions are not very flexible and have no TYPO3 inside-knowledge so the TYPO3 agencies n@work/Hamburg and networkteam/Hamburg+Kiel teamed up to create the specific TYPO3 monitoring system caretaker.

Development targets:

- Easy management of tests (monitoring of a specific function) with the TYPO3-Backend
- Secure monitoring of distant TYPO3-installations
- Inclusion of integration-tests
- Good extendability of the whole System

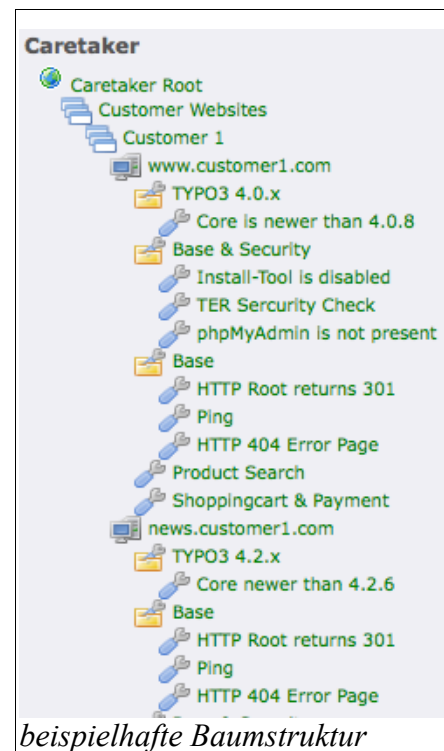
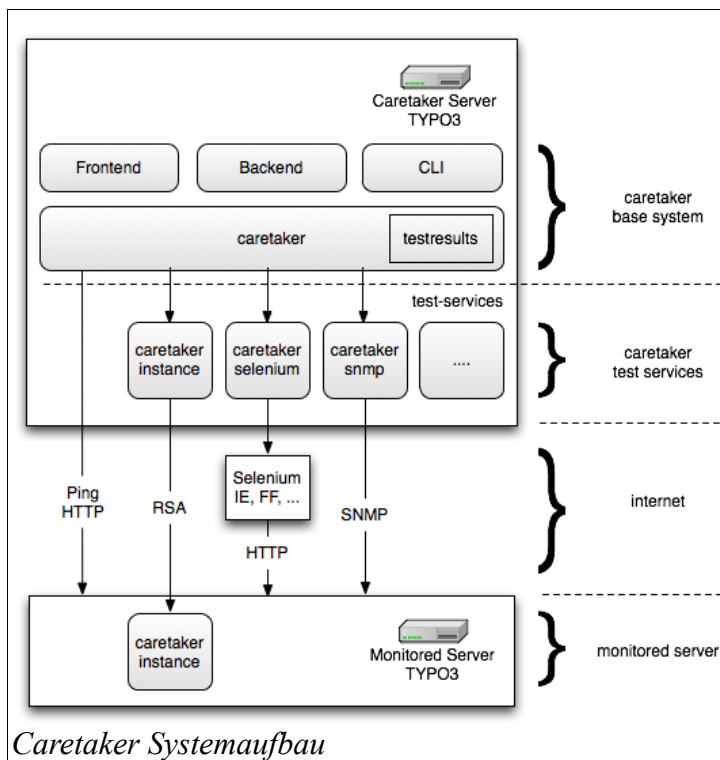
## 2 The Caretaker TYPO3-Extension

Based on that targets we created the TYPO3-extension caretaker which is the core of our monitoring-system. Caretaker is responsible for the central management, execution of tests and the storing an aggregation of testresults. For test execution and monitoring of test-states we created a backend module and a cli-interface. Usually the cli interface will be used to execute the tests on a regular basis via cron. The backend-module will show the state of the system and will allow the administrator to re-execute tests when errors are fixed. For each test the interval and the addresses for error notification can be configured. For customers and non-admins a frontend-plugin is included which can give a short overview about the current system-state.

The base of system monitoring with caretaker is, like with any other monitoring solution, the infrastructure monitoring. Therefore SNMP (Simple Network Management Protocol), Ping and HTTP Tests can be defined. Additionally we'll implement the access of nagios sensors via NRPE (Nagios Remote Plugin Executor) in the near future.

### 2.1 Monitoring remote TYPO3-Instances

A speciality of monitoring TYPO3-installation with caretaker is the possibility to automate TYPO3 security checks. After installing the extension caretaker\_instance on the server and the remote system you have the option to create tests for TYPO3-core and extension versions. The extensions tests can be configured to automatically detect extensions which are not from TER or which are marked insecure. In future we will also integrate tests for password quality and for the detection of unwanted or inactive user accounts.



It is important to point out that the management of security tests only happens once on the server. Afterwards many TYPO3-installations can be checked with the same rules. To prevent unauthorised access to system informations the whole communication is rsa encrypted with public/private keypairs for each affected system. Additionally the interface only allows access to some predefined, reviewed and readonly methods.

## 2.2 Integration Tests

To support integration tests we integrated the open source project Selenium. Selenium is a Java application which is starting a browser with some additional javascript to simulate the user interaction. The Java base enables Selenium to run on all important operating Systems and to remotely control a wide range of Browsers. Even Internet Explorer is supported in version 6,7 and 8. The extension caretaker\_selenium integrates Selenium into caretaker defines an interface for test managing. Important is that those tests are based only on the DOM and so cannot detect layout errors.

## 2.3 Extendability

All available test-methods are implemented as TYPO3-services. The service list can be easily extended by TYPO3-extensions. That's why the caretaker base only contains simple tests for HTTP and PING. Adding new test-services is simple. You only have to implement a single Method (runTest) and provide a flexform configuration file.