Semantic MediaWiki as an Integration Platform for IT Service Management

Frank Kleiner, Andreas Abecker

FZI Forschungszentrum Informatik
an der Universität Karlsruhe (TH)
{kleiner, abecker}@fzi.de

Abstract: We describe our work on using Semantic MediaWiki as a central platform for managing IT services and the underlying technical components within an organization. We present our toolkit of MediaWiki extensions which add ITSM-specific functionalities to Semantic MediaWiki and describe their interactions. We also outline the benefits gained by using Semantic Technologies in IT Service Management.

1 Introduction

IT Service Management (ITSM) deals with providing reliable IT services. The perspective of ITSM is customer-centric which distinguishes it from more technology-oriented IT management approaches of the past. This customer focus helps to ensure the alignment of services provided by the IT department with the business goals of an organization [Add07]. The IT Infrastructure Library (ITIL) is the most widely used ITSM framework. ITIL consists of five volumes which form a lifecycle encompassing all aspects of an IT service. Our work focusses on the aspects of Configuration Management and Change Management [LM07] as well as Problem and Event Management [CW07]. Configuration Management deals with providing a system in which all relevant items for providing services are stored, together with their interactions with each other. Items represented in the Configuration Management System (CMS) are referred to as Configuration Items (CIs). Change Management focusses on providing processes and procedures for planning changes in order to minimize the associated risks of failed changes or unwanted side effects. Problem Management deals with finding and fixing the causes of malfunctions in components which impact the working of services. Event Management is concerned with monitoring the working of IT services and the underlying technical components as well as reporting of failures or potential problems.

Wikis [EGHW07] are Web-based platforms which enable users to edit articles from within their Web browsers. This makes Wikis a perfect platform for the collaborative generation of knowledge, as exemplified in Wikipedia1, the world’s largest encyclopedia. Within organizations, Wikis are more and more often used for collaborative knowledge manage-

1http://www.wikipedia.org
ment. **Semantic Wikis** [SBBK09] extend Wikis by semantic features which enable them to use ontologies [SS09] as the underlying data model; this makes available additional mechanisms for representing, organizing and retrieving information. Semantic MediaWiki (SMW) is an extension for the popular MediaWiki [Bar08] platform. It allows to give meaning to links between articles by enabling users to explicitly describe their semantics. Attributes can be used to state fact knowledge in Wiki articles which can be processed within SMW or by external reasoners. Class hierarchies can be built by using MediaWiki categories. [KVV+07] describes SMW in detail and gives examples.

**Problem description and approach:** Professional ITSM requires processes for the management of configuration items, for the structured application of changes, as well as for diagnosing problems and for monitoring services and hardware components for events that indicate malfunctions. Software tools help system administration personnel to run these processes. While very small IT environments usually are fine with a few text or spreadsheet documents describing the functions of components and common problems, large IT environments use specialized commercial software which in most cases is expensive and whose maintenance is labour-intensive. This paper gives an overview of our Semantic ITSM Wiki which was introduced in [KA09]. It addresses the following challenges: (1) provide an extensible platform, built on top of freely available software, for managing medium-sized IT environments; (2) enable computer-savvy non-administrative users to collaboratively contribute to the ITSM Wiki; (3) provide extensions for automatically adding information from managed components, integrating a systems monitoring tool and a network intrusion detection system into the ITSM Wiki, as well as providing a mechanism for supporting administrative personnel in tracking down hardware and software problems.

The **structure of the paper** is as follows: Section 2 gives an overview of our extensions which extend the Semantic MediaWiki platform by ITSM-specific components. Section 3 surveys some related work. Section 4 concludes and sketches some future work.

## 2 ITSM Extensions for Semantic MediaWiki

The goal of the authors’ ongoing work is to extend the Semantic MediaWiki platform by extensions for the use in the ITSM area. Semantic Wikis provide a platform which combines the ability to store structured information in the form of relations and attributes with the ability to store free text. In the context of ITSM, this enables the storage of, for example, dependencies between services and computers in the form of relations, together with documentation in the form of free text. The following subsections present four extensions which address four of the most commonly implemented ITSM processes. The most implemented processes are Incident Management including the Service Desk function, as well as Configuration Management, Problem Management and Change Management (cp. [BT05]). The authors have decided not to implement the Service Desk function at the moment because of the use of the OTRS tool in their environment\(^2\).

\(^2\)http://www.otrs.org
Population with Static and Dynamic Information: In order to have available always up-to-date information about the status of IT components (e.g., computer configurations, including the installed hardware and software), it is imperative to have a mechanism for automatically gathering the needed information, because manually gathering information is both time consuming and error-prone. The component described in more detail in [KAL09] implements a mechanism for remotely collecting information over the network from Windows computers via the Windows Management Instrumentation (WMI) mechanism [Jon07]. This enables ITSM Wiki users to always access the current version of configurations, including information about hardware and software (e.g., installed applications). Furthermore, a component for reading and writing configuration information via the Simple Network Management Protocol (SNMP) [Sch05] was implemented which extends the range of devices from which information can be gathered to network-enabled hardware components, e.g., printers and network switches.

Generating Systems Monitoring Information: Monitoring IT components for their correct behavior is important for providing a high level of service quality. If a service stops working, correct measures must be initiated, ranging from automatically restarting the troubled service to alarming the administrator who is responsible for the correct working of the service. In ITIL, systems monitoring is part of the Event Management process which is described in the Service Operation volume [CW07]. The Systems Monitoring component, previously described in more detail in [KAB09b, KAB09a], builds on top of the Nagios [Bar05] systems monitoring tool which can be configured to monitor networks of almost all sizes and complexities. The Systems Monitoring extension integrates Nagios into the ITSM Wiki by allowing to register Wiki articles which represent Configuration Items (i.e., computers, or networking equipment) to be monitored by the external monitoring tool. Semantic relations which are used to represent relations between CIs, are converted into service dependencies within Nagios. This frees the administrative staff from separately maintaining a systems monitoring configuration and enables them to access systems monitoring information from a unified user interface.

Integration of Intrusion Detection Information: Monitoring systems for security incidents is accomplished by implementing an intrusion detection system infrastructure. Depending on their location, intrusion detection systems can be differentiated between network intrusion detection systems and host-based intrusion detection systems. Our work builds on the signature-based network intrusion detection system Snort [Roe99]. Signature-based network intrusion detection systems capture network traffic and use signatures for checking if it contains malicious data (cp. [Koh06]). In [Axe00], it is shown that intrusion detection systems have an inherently high rate of false positives because of the high amount of non-malicious traffic in contrast to the amount of malicious traffic. The integration of the Semantic ITSM Wiki with an external intrusion detection system helps to minimize the number of false positives by taking into account semantic facts stored in the Wiki. By using the ITSM Wiki as the user interface for displaying potential intrusions, semantic features are made available (e.g., the dynamic creation of a customized filter for finding certain network traffic). A filter between the Snort database and the Wiki only imports information which is classified as potentially malicious to the target system. An example for a potential attack which is recorded in the Snort database due to the lack of
background knowledge, but not imported into the ITSM Wiki, is the following: an attack is detected which tries to exploit a security hole in the Microsoft Internet Information Server (IIS), but on a server running Apache under the Linux operating system. The attack is logged into the the Snort database. While it would be presented to the administrator when using a standard program (e.g., BASE³) for displaying events, the Intrusion Detection extension acts more intelligently. It checks whether the system against which the attack is targeted, is indeed susceptible to the attack. Because the facts stored in the Wiki show that the system is running Linux, it is deduced that it cannot be running IIS and thus cannot be attacked by an exploit targeted at IIS. By reducing the number of false positives, administrative personnel can concentrate on real attacks, which leads to an improvement in overall systems security.

**Semantic Problem Finder:** Problems in ITIL are defined “as the unknown cause of one or more incidents” [CW07]. In order to deliver reliable IT services, efficient processes and tools for tracking down problems have to be present. The Semantic Problem Finder, which is implemented as a MediaWiki extension, provides tool support for administrators to help locate the underlying cause of problems. By using the SMW-based semantic Configuration Management Database as a foundation, possible common causes for a set of given problems are determined and given to the administrators for review. The process for finding the cause of a problem is as follows: (1) a problem is reported to the administrative staff; (2) an administrator enters the affected configuration items into the Semantic Problem Finder extension; (3) a list of possible causes is determined by building trees which represent connections and dependencies between CIs. The following (trivial) example helps in clarifying the process: (1) a problem is found which prevents multiple computers from connecting to the network; (2) the names of some or all of the affected computers are entered into the Problem Finder; (3) it can be seen that all computers are connected to the same network switch which with high probability is the cause of the problem.

### 3 Related Work

There exists a number of tools supporting administrative personnel in providing IT services. Specialized tools for managing Configuration Management Databases are Peregrine, i-doit, and OTRS::ITSM. Being built for managing structured data, the flexibility of these tools does not reach the flexibility provided by a Semantic Wiki as the technical foundation. Tools for automatically gathering information from computers over the network are available from commercial vendors and as Open Source. The software Spiceworks⁴ is an example for a specialized tool for asset and configuration management which automatically reads configuration data over the network. By transferring automatically gathered information into semantic relations and attributes, the extension created by the authors makes possible features which exceed the functional range of classic tools, e.g., much more flexible, complex queries. Tools for managing systems monitoring configurations for Nagios are Lilac Configurator, Monarch and NCPL. A tool for displaying and

---

³http://base.secureideas.net/
⁴http://www.spiceworks.com/
filtering intrusion detection data is BASE, which is a Web-based front-end for accessing Snort databases. In [HO09], the benefits of using a Semantic Wiki for managing metadata are quantified, which is related to the approach presented in this paper, which uses a Semantic Wiki for managing metadata about IT infrastructures. In [Lan10b, Lan10a], a Semantic Wiki-based helpdesk and data center inventory system is described, which in some aspects can be compared to the work presented in this paper.

4 Summary and Future Work

We summarized our ongoing work on building an integrated platform for the management of IT services and infrastructures on top of a Semantic Wiki. In order to enable administrative staff to gain productivity from the use of the Semantic Wiki, four specialized tools were presented which are implemented as MediaWiki extensions. The first tool collects data from computers and other components over the network and integrates the information in the form of semantic facts into the Wiki. The second tool integrates an external systems monitoring tool, while the third one builds an interface for importing information from an external intrusion detection system. Finally, the fourth one helps in tracking down problems by looking for common causes in tree data structures generated from semantic facts. While parts of the system described in this paper are running in a productive environment consisting of 500 computers, a formal evaluation of the benefits gained from the use of a Semantic Wiki as a hub for all information relating to IT Service Management within an SME company, will be done in the future. Furthermore, a component for integrating an external Service Desk tool (e.g., OTRS) is planned.

References


