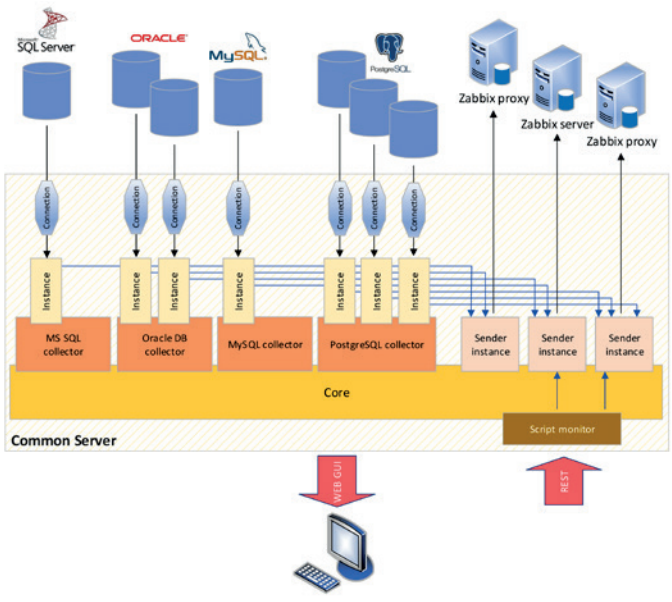
Axians Slovakia – author of extensions and modules for the Zabbix monitoring tool

Axians Slovakia is the author and supplier of several accessories for the Zabbix monitoring tool. Our extensions and modules are developed for heterogeneous environments and support a wide range of operating platforms (Linux, HPUX, Solaris, AIX, MS Windows). New functionalities of the Zabbix product are used, such as global correlation or the enrichment of generated incidents (Zabbix event tags). The offered implementation of extensions and modules consists of seven groups:

- Monitoring of a heterogeneous database environment (Oracle, MS SQL, PostgreSQL, MySQL, MariaDB, Galera) – **Common Server** module
- Service tree creation – **BSM** (Business Service Management) module
- Monitoring of SAP ERP environment via CCMS – **SAP** module
- Monitoring of log files and SNMP traps – **TBC** (Time Based Correlation) module
- Monitoring of large heterogeneous server environments at the OS level – **Prefabricated** module
- Central repository of monitored server configurations, distribution configuration and remote administration of Zabbix agent and Zabbix proxy – **Distribution System** extension
- Timer for automatically closing incidents

All extensions and modules come in the form of open source scripts, configuration files and Zabbix templates without licensing restrictions. The customer can freely modify and use the delivered solution. The delivery includes detailed installation and administrative documentation.

The modules and extensions can be adapted to the specific needs of the customer and, if required by the customer, training is also provided.



Common Server architecture

DATABASE ENVIRONMENT MONITORING – COMMON SERVER MODULE

The Common Server module provides the possibility of fault and performance monitoring of a heterogeneous database environment (Oracle, MS SQL, PostgreSQL, MySQL, MariaDB, Galera) with the following functionality and features:

- **Agent less monitoring** – the module does not use Zabbix agents, but transmits data via the Zabbix sender tool collected using its own collectors created for individual types of databases with the possibility of encrypted communication
- **Simple and unified configuration of data collection from databases** - the monitoring of each database instance using its collector is described by a separate or shared configuration file or files offering the following settings:
  1. Autodiscovery of metrics from data in the database
  2. Timed data collection based on defined intervals
  3. Thresholds defined for metrics listed directly in the configuration file or using values in the database
  4. Setting up the enrichment of generated problems using static data specified directly in the configuration file or using values in the database
- **Self monitoring:**
  1. Monitoring of the success and time for obtaining the individual monitored values
  2. Monitoring the activity of individual instances of the Common Server and its collectors (RAM, CPU)
- **Event tables** – collection and subsequent correlation of events presented by the content of a specific table or tables (this functionality ensures the functioning of Zabbix integrations with specific event sources, which take the form of records in selected database tables)
- **Script monitor** – execution of any scripts via the REST interface, the output of which is passed to Zabbix together with monitoring the duration and success of their convergence
- **Web GUI** – each instance of Common Server has its own web interface, which can be used to manage all its common components and view the deployed configuration
- **Collector health** – dashboard presenting the status of a specific collector instance (RAM, CPU, duration of data collection, database and collector version)
- **Jednoduchá inštalácia** – Common Server is a group of scripts written in Python. Python Interpreter and a group of Python modules are needed.

In a monitored environment, an arbitrary number of instances of a common server can be used, and each can use a number of instances of collectors that actively monitor several different types of databases and send data to different target Zabbix proxies or Zabbix servers.

Axians Slovakia s.r.o., Plátennícka 19013/2, 821 09 Bratislava
Tel.: +421 258 273 111, E-mail: axians@axians.sk
www.axians.sk

ZABBIX PREMIUM PARTNER

Main Senders **Collectors** Script Monitors Connections Logout Instance: CommonEngine1 s&t

Refresh | Rescan configuration directory

Name	Connection name	Connection type	Sender name	Zabbix host	Check files	Run On Startup	Load Info	Note	State	Actions
mssql1	mssql_win	MSSQL	remote_server1	**mssql.test01** (from sender)	config/checks/mssql_standard1.cfg Show	No	config/collectors/mssql1.cfg --- 2019-05-12 22:55:21		RUNNING since 2019-05-27 13:09:27	Stop
mssql2	mssql_win	MSSQL	local_server5	**MSSQL.database1** (from sender)	config/checks/mssql_standard2.cfg Show	No	config/collectors/mssql2.cfg --- 2019-05-23 17:36:47		RUNNING since 2019-05-27 13:09:29	Stop
mysql1	mysql_zabbix	MYSQL	local_server3	**MySQL.database1** (from sender)	config/checks /mysql_master_standard1.cfg Show	No	config/collectors/mysql1.cfg --- 2019-05-17 19:42:50		RUNNING since 2019-05-27 13:09:30	Stop
oracle1	oracle_local_dev	ORACLE	local_server1	**OpenView.database1** (from sender)	config/checks/oracle_standard1.cfg Show	No	config/collectors/oracle1.cfg --- 2019-05-12 21:50:12		RUNNING since 2019-05-27 13:09:32	Stop
oracle2	oracle_local_dev	ORACLE	local_server2	**OpenView.database2** (from sender)	config/checks/oracle_standard2.cfg Show	No	config/collectors/oracle2.cfg --- 2019-05-12 21:50:51		RUNNING since 2019-05-27 13:09:34	Stop
pg1	postgres_local_dev	POSTGRES	local_server4	**PG.database1** (from sender)	config/checks/pg_standard1.cfg Show	No	config/collectors/pg1.cfg --- 2019-05-12 16:27:28		RUNNING since 2019-05-27 13:09:35	Stop

Common Server 1.0.2 © 2019, S&T Slovakia

Common Server module GUI web – presentation of collector activity

CREATING A SERVICE TREE – BSM MODULE (BUSINESS SERVICE MANAGEMENT)

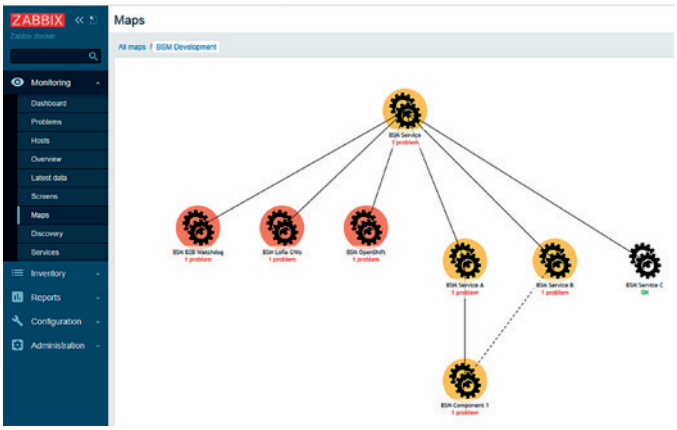
The BSM module is a unique solution for modeling and presenting the state of services through a service tree with a number of important functionalities that bring Zabbix to the level of commercial monitoring tools:

- Graphical presentation of the service tree
- **Calculation of the state of services (nodes of the service tree) based on the propagation of states between the nodes of the tree and the binding to events using tags!**
- Binding of tree nodes to:
  1. All problems
  2. Acknowledge problems
  3. Suppressed problems (planned outages)
- Notifications from service tree nodes when their status changes
- SLA evaluation based on service severity
- Root Cause Analysis (RCA)

Implementing the module is simple as no third-party tools, databases, or configuration files are required. The entire configuration is part of the Zabbix configuration and for backup purposes it is sufficient to back up the Zabbix database.

Benefits of the BSM module:

1. Immediate overview of the status of services provided by the company's IT environment
2. Ability to present the impact of outages on business processes
3. Direct notification (SMS, mail...) only in case of a change in the status of specific services within the competence of a specific manager
4. Immediate information on the status of SLA fulfillment for any period (day, week, month, year)
5. RCA – identification of events that are responsible for the malignant state of the service and subsequent access to specific metrics for the purpose of finding the cause



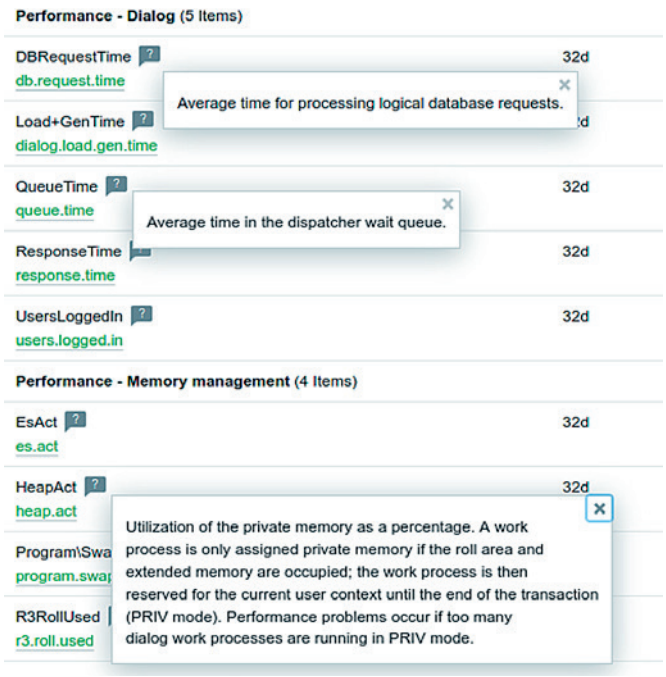
Graphical presentation of a part of the service tree in a graphical interface

Axians Slovakia s.r.o., Plátennícka 19013/2, 821 09 Bratislava
Tel.: +421 258 273 111, E-mail: axians@axians.sk
www.axians.sk

ZABBIX PREMIUM PARTNER

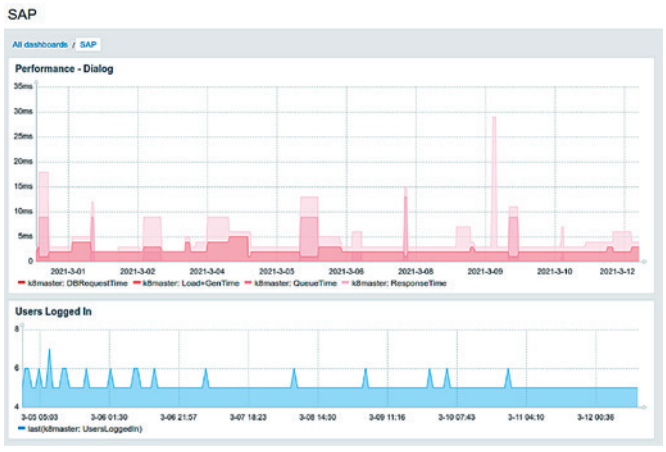
MONITORING OF SAP ERP ENVIRONMENT VIA CCMS – SAP MODULE

Through the integration with the CCMS (Computing Center Management System), Zabbix enables the collection and evaluation of metrics from individual instances of SAP systems. In this way, the central so-called "Umbrella" view of the company's IT infrastructure is available in one place in the Zabbix tool. The CCMS tree provides a number of metrics (hundreds) not just about the status of a particular SAP instance, but also about its performance.



Examples of performance metrics

The prerequisite for data collection is an SAP user with a password and a role that allows access to CCMS data. The integration can be installed directly in the system together with the Zabbix agent or it can be installed using a Zabbix proxy (remote data collection). The solution is built and delivered with open code together with instructions that allow the creation of specific metrics according to the customer's needs and their visualization through dashboards.

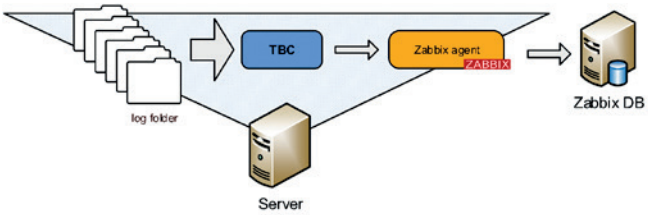


Dashboard example for SAP module

MONITORING OF LOG FILES AND SNMP TRAPS – TBC MODULE

The TBC (Time Based Correlation) module provides detailed monitoring of a large volume of log files and SNMP traps. The module allows the following:

- Monitoring using Zabbix agent (log files) and Zabbix proxy (SNMP traps) – **no additional applications or databases need to be installed**, the module consists of one script and its configuration files defining the so-called correlators
- **Monitoring of individual log files or entire directories** – it is enough to define a directory and its entire content will be monitored, including subdirectories or a part thereof (log files can be freely created and removed in directories)
- **Monitoring of log files with multiline records**
- **Ability to configure any correlation and filtering rules** already at the level of Zabbix agent or Zabbix proxy - only correlated and filtered records flow into the Zabbix database, which should be the basis for incidents. The delivery includes several most frequently used rules in the form of correlators:
  1. **Suppresing** – suppression or release of selected types of records/traps
  2. **Repeating** – release of the record/trap if the defined number of its repetitions is reached
  3. **Time suppresing** – suppression of selected types of records/tracks in a defined time interval
  4. **Inhibition** – release of the record/trap if no other defined type of record/trap appears within a defined time interval
  5. **Storm detection** – release of the record/trap if no other defined type of record/trap appears within a defined time interval
- **Counting of duplicates** – all correlators also count the number of occurrences of a certain type of record/trap in order to present the number of duplicates of individual types of incidents in the Zabbix environment.
- **Self monitoring** – monitoring of the TBC module within individual Zabbix agents and Zabbix proxies



Implementation architecture of the TBC module for monitoring directories with log files

Axians Slovakia s.r.o., Plátennícka 19013/2, 821 09 Bratislava
Tel.: +421 258 273 111, E-mail: axians@axians.sk
www.axians.sk

ZABBIX PREMIUM PARTNER

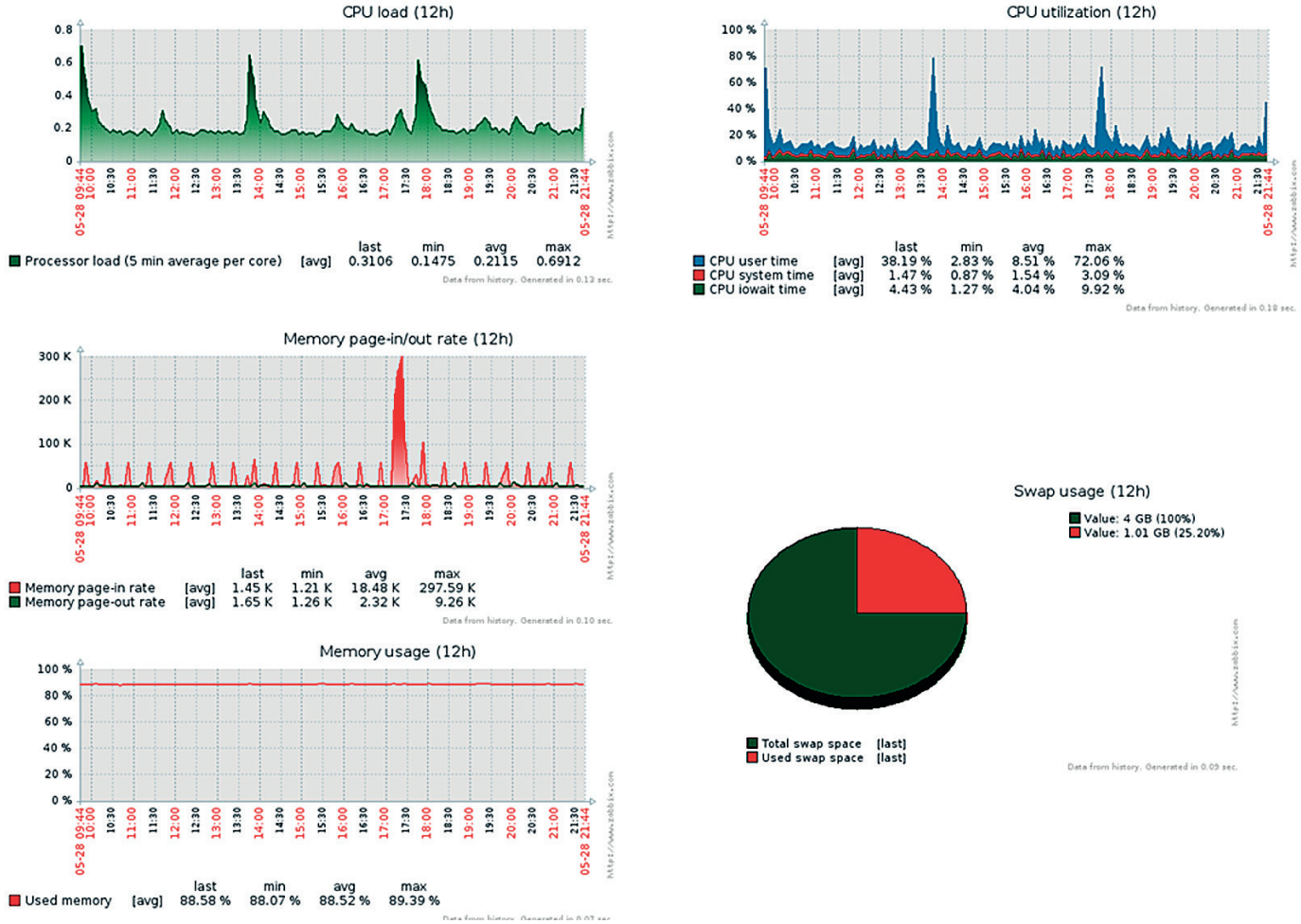
MONITORING OF SERVERS AT THE OS LEVEL – OS MONITORING MODULE

The module simplifies and accelerates the deployment of monitoring and its administration at the OS level for large numbers of servers in heterogeneous environments as well as in **active/passive and active/active** cluster configurations. The module allows you to configure the monitoring of processes, services, network sockets, connections and file system occupancy using only simple configuration files designed for a specific server, **without the need to take action in the graphical interface of Zabbix or restart any of its components**. The module provides monitoring for the following:

- **running of processes and services** – kconfiguration of monitoring the running of processes and services; the process or service run, the account under which it runs, and the number of instances are monitored
- **status of sockets and connections for TCP/UDP protocols** – the activity of sockets is monitored, as well as entire connections in the case of TCP (LISTEN, ESTABLISHED statuses...)
- **occupancy of local and network file systems** – the free space of the file systems is monitored in percentages as well as in megabytes; thresholds are given for two severity levels directly in the configuration files; the file system status is also monitored (disconnected/mounted).

The module provides monitoring for performance metrics (e.g. CPU, RAM, SWAP), the set of which can be freely supplemented. The threshold configuration is created using Zabbix macros.

In the configuration files, it is possible to specify e.g. the name of the service, the severity of the incident being opened, or create additional attributes by which open incidents in the Zabbix environment will be enriched in the form of so-called Zabbix event tags.



Example of a screen (Zabbix screen) generated by the Prefabricated module

Axians Slovakia s.r.o., Plátennícka 19013/2, 821 09 Bratislava
Tel.: +421 258 273 111, E-mail: axians@axians.sk
www.axians.sk

ZABBIX PREMIUM PARTNER

CENTRAL CONFIGURATION REPOSITORY – DISTRIBUTION SYSTEM EXTENSION

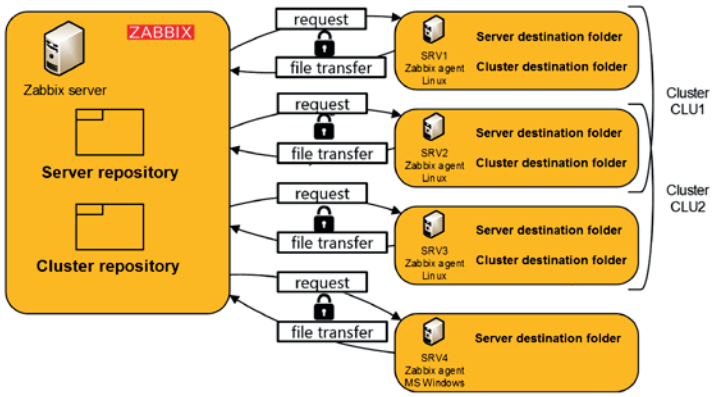
The extension complements the functionality of Zabbix **with the ability to create a central repository or repositories to configure agents of monitored servers in order to distribute them to individual servers or entire clusters in a heterogeneous environment**. The distribution system allows you to distribute monitoring scripts or binaries that extend the functionality of Zabbix Agent or Zabbix Agent2, monitoring script configuration files, or Zabbix Agent configuration files. The extension also allows the remote management of Zabbix agents and Zabbix proxies. Thus, supervisors do not need to directly access the monitored servers in the process of configuring and changing the monitoring. The following tasks can be performed remotely for all monitored servers:

- execution of a command on the monitored server
- listing of agent configuration files on the monitored server
- distribution of repository content to a monitored server or cluster
- listing of the current contents of the distribution directory on the monitored server
- status detection, stop, and restart Zabbix agent on the monitored server
- status detection, update, stop and start Zabbix proxy

All the above tasks can be performed from Zabbix GUI or using CLI tools, which can be used to create your own scripts.

It is not necessary to install any additional agent, create new accounts or open additional ports on the firewall on the monitored servers, as Zabbix agent or Zabbix agent2 is used and communication is secured by encryption.

The extension is open and can be supplemented with new functionalities and tools. For example, in the case of using the OS monitoring or TBC module, the delivery of the Distribution System also includes tools for the remote management of these modules.



Example of implementing the Distribution System extension

TIMER FOR AUTOMATICALLY CLOSING INCIDENTS

The module allows you to set the validity period at the level of a Zabbix trigger for the incident it opens. After the set time has elapsed, the incident will be closed automatically. The validity can be defined by the number of days or hours. **This solution will ensure the automatic closure of incidents even if there is no automatic corrective condition or action for the given type of incident**.

The automatic timed closure configuration complements other incident closure techniques that may cœxist with it – that is, a particular incident may be closed by more than one situation/condition, depending on which situation/condition occurs first:

- The cause of the incident has disappeared
- Incident deduplication
- The incident was manually closed by the operator
- The incident was closed after the set validity period

Axians Slovakia s.r.o., Plátennícka 19013/2, 821 09 Bratislava
Tel.: +421 258 273 111, E-mail: axians@axians.sk
www.axians.sk

ZABBIX PREMIUM PARTNER