

Support Centre

FEATURES:

- 24/7
- Real-time Monitoring
- Short response time
- High level of security
- ISO 27001 certified



Customer care of MicroStep-MIS goes beyond deployment of a working solution. Through wide range of technical support and maintenance facilities, we can proactively support all customers, with minimal effort on their side.

Our Support Centre is responsible for real-time monitoring of all customer systems in the world, so we can detect and fix all the possible issues immediately. In order to achieve this objective, we have built a comprehensive monitoring system. Furthermore, our support team is receiving all important issues from logs and the current server condition by e-mail on daily basis.

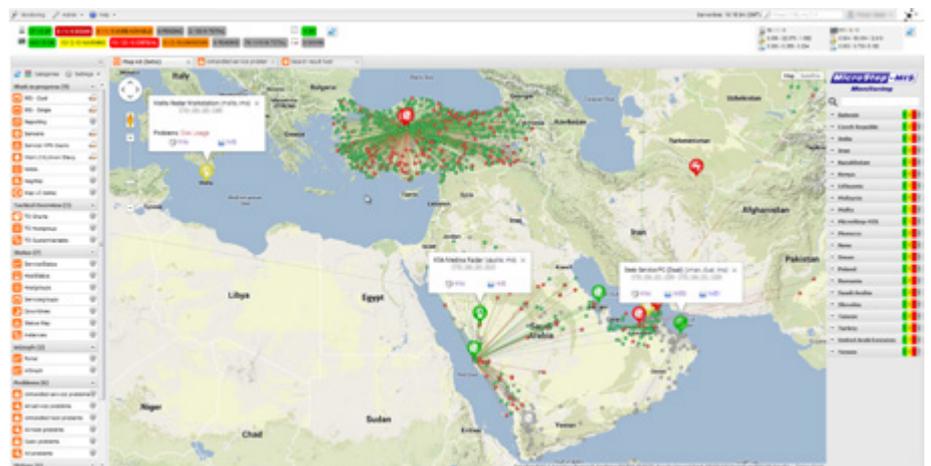
Central monitoring

The map overview is great for both global and detailed view of the current status of client systems.

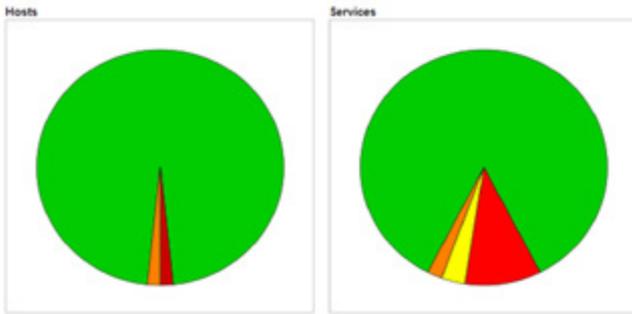
As soon as a problem occurs, the color of its icon changes, depending on the type of the issue. All the details needed to solve the particular problem are immediately available, including the project documentation.

We are monitoring every network service and every important resource of the deployed servers. In order to track down the issues from the past, we also store the status history for every operation and graphs of historical values for server's resources. (e.g. CPU, RAM or disk usage).

One does not have to be an IT professional to benefit from our monitoring. We are able to publish relevant reports, open parts of our monitoring system to our customers or even build their own monitoring infrastructure.



» Map overview zoomed to a few of customer systems



» Tactical Overviews

Host name	Service name	State	Last Check	Duration	Output	Service Information
Server01	SMTP Connection	OK	2014-05-21 10:14:20	00:00:00.00	SMTP (SMTP) 1.28 (0) - HELO/STARTUP OK (200 OK)	
File Server	CPU Load	OK	2014-05-21 10:17:20	00:00:00.00	OK - load average: 0.02, 0.05, 0.10	
DB 1	MySQL Status	CRITICAL	2014-05-21 10:16:20	00:00:00.00	MySQL - MySQL (1) 10000000 (0% loaded/0%)	
DB 2	MySQL Status	CRITICAL	2014-05-21 10:16:20	00:00:00.00	MySQL - MySQL (1) 10000000 (0% loaded/0%)	

» Icinga Classic Web Interface on customer's system

IMS Status ERRORS: Communication, CPU Load, Memory, Network Interfaces. WARNINGS: Distribution

Status Details

Label	Status
Communication	WARNING
Distribution	WARNING
Database	OK
MySQL Status	CRITICAL
Processes	OK
MySQL Restart	OK
OS Uptime	OK
CPU Load	WARNING
Memory	WARNING
MySQL	OK
Hard Disk Drive	OK
Software RAID	OK
Network Interfaces	ERROR
User Messages	WARNING
Log Files	OK

» BITE screen (Icon and Table View) in IMS

Local (on-site) monitoring

Our systems are deployed with extensible built-in tests, so any issue disrupting normal system operation can be detected and resolved in no time. Users can access comprehensive BITE screens directly from the web browser, which enables them to have a clear overview on the current situation. External monitoring systems (such as OpenNMS, IBM Tivoli, HP OpenView, Icinga, Nagios...) can be interconnected through industry standard SNMP protocol.

In case of complex structure of customer's site that consists of multiple systems, we deploy additional layer of monitoring. This way we are able to monitor the current status of all the systems from a single point. There is also a possibility to connect our system to customer's existing monitoring solution.

By far, the most popular and extensible solution is Icinga. Icinga is the modern open-source fork of Nagios the standard system monitoring solution. The key to the success of Nagios is simplicity and extensibility. Virtually anything can be monitored, as long as there is a possibility to execute the "check" in the Linux or Windows environment.

Security

With such an extensive monitoring, several procedures had to be put in place to address security, confidentiality, extensibility, stability and performance.

In order to mitigate all the possible threats, our monitoring is entirely based on read-only SNMP access, which can not be used to remotely access a computer, spread unauthorized code (malware), or to disrupt any of its functionality. It is also easily extensible, because no special monitoring agents have to be set up on monitored systems.

SNMP has become an industry standard for network monitoring, due to its performance, which is based on UDP. To protect the confidentiality of information and stability of connection all the monitoring communication is tunnelled through our Open VPN SLA network.