

Open Source Client Management System opsi



opsi Nagios Connector

The opsi Nagios Connector

This substantial extension of the opsi web service and the opsi client agent allows to connect the opsi managed windows clients and the opsi server to Nagios/Icinga monitoring services.

Motivation

Not primarily being a monitoring tool, opsi can be used as an interface to provide Nagios monitoring services for Windows clients. Additionally, the performance of opsi itself can be monitored.

Therefore opsi offers an interface to Nagios (or Nagios related) monitoring services.

By providing a monitoring interface, this opsi extension is a big step to put ITIL concepts into practice.



Provided Services

The *opsi Nagios Connector*

- provides monitoring functions for the opsi server
- checks software rollouts
- monitors client states

Integrated Monitoring

Requests for monitoring information are sent via a secure (https) channel to the opsi web service, which verifies request authentication before responding.

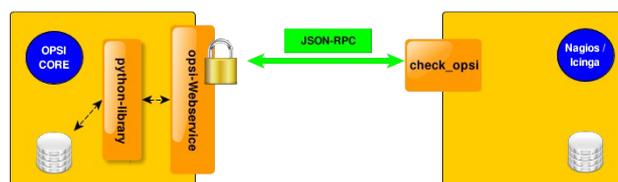
The monitoring data remain encapsulated on the opsi server, which is a significant security advantage and also simplifies the Nagios/Icinga configuration.

The opsi web service receives the information requests and returns only the summarized results as configured. Besides of the security advantage, this approach helps to reduce network load, so that even large networks can be checked at short time intervals.

There are several types of checks available:

Indirect Checks

Indirect client checks deliver information based on the opsi backend data. They do not require that the client is currently running.

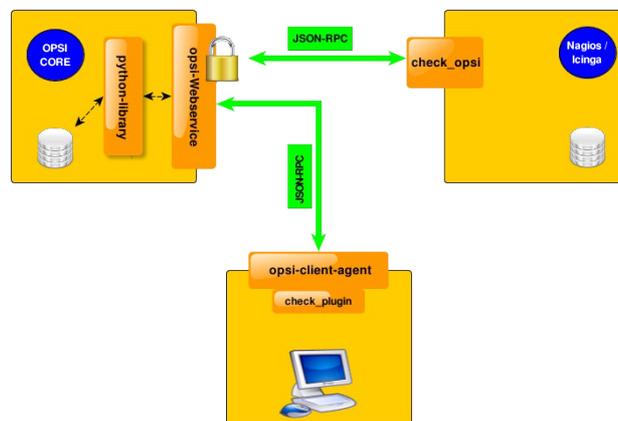


E.g. you can use an indirect check to monitor the opsi client state: this may tell you, whether a specific product is rolled out successfully, or if there is some product waiting to be installed, or if any install action failed.

Direct Checks

Direct client checks are executed directly on the client using the existing opsi-client-agent as a kind of Nagios agent

One application of this feature is cross checking data managed via the opsi service. E.g., you may test if the signature file of the antivirus software really is the current one, or verify that the antivirus software is not deactivated.



Since the opsi server is working as an intermediate agent, there is no need that the monitoring server itself has authentication privileges for the opsi clients.

Data management by the opsi server gives the additional advantage that status information is permanent available, even when the client is not running anymore. If e.g. a problem concerning the antivirus software occurred, the service keeps the status *CRITICAL* as long as the service does not get new data from the client. In a conventional monitoring scenario, the client state would change to *UNKNOWN* when the client is shut down, although the problem was not solved.

Deployment and administration of monitoring plugins is easily managed by the standard processes and tools of the opsi client management.

Usage Examples

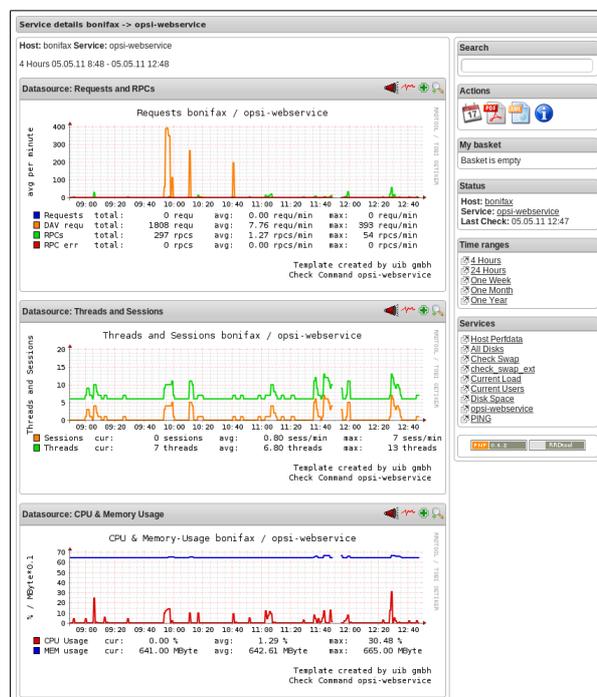
The *opsi Nagios Connector* may be used e.g. for

- ➔ opsi web service status reports (including performance data)
- ➔ client state checks
- ➔ state checks for host groups
- ➔ checks for product states
- ➔ checks for state of product groups
- ➔ checks of depot server synchronization
- ➔ direct checks on the opsi clients

Server				Test clients			
Host	Status	Services	Actions	Host	Status	Services	Actions
dplaptop	PENDING	1 OK 2 WARNING 2 CRITICAL	[Actions]	depotclient.svm.local	PENDING	1 CRITICAL	[Actions]
				pxcellent.svm.local	PENDING	1 UNKNOWN	[Actions]
				svmclientde.svm.local	PENDING	1 UNKNOWN 2 CRITICAL	[Actions]
				svmcclientxpint.svm.local	PENDING	1 UNKNOWN	[Actions]
				svmvista.svm.local	PENDING	1 OK	[Actions]
				svmvpnclientde.svm.local	PENDING	1 UNKNOWN	[Actions]
				svmw7x64.svm.local	PENDING	1 UNKNOWN	[Actions]
				test-0.uib.local	PENDING	1 CRITICAL	[Actions]
				test-1.uib.local	PENDING	1 WARNING	[Actions]
				test-10.uib.local	PENDING	1 WARNING	[Actions]
				test-100.uib.local	PENDING	1 WARNING	[Actions]

Summary

- ➔ The *opsi Nagios Connector* module comes with a single plugin on the monitoring server. All the complex monitoring procedures are contained within the opsi web service.
- ➔ There is no additional agent required for direct checks on opsi clients.
- ➔ Monitoring in large or distributed networks can be scaled more efficiently than by using stand alone Nagios checks.
- ➔ Deployment and administration of monitoring plugins are easily done via the opsi client management processes.
- ➔ There is a direct red/green monitoring of the complete opsi status (configserver, depotserver, opsi clients etc.)



Cofunded Development

The *opsi Nagios Connector* module is realized as a cofunded opsi extension project.

More about cofunded opsi extensions:
http://uib.de/en/opsi_cofunding/cofunding

Contact

Please visit us at the opsi.org project web site <http://www.opsi.org>, or for commercial support at <http://uib.de/en/support-training/support/>



uib gmbh ▪ Bonifaziusplatz 1B ▪ D - 55118 Mainz
 Phone: +49 6131 / 275610 ▪ info@uib.de