

Monitoring und Ausfallsicherheit

Systemwächter

Störungen innerhalb der IT-Infrastruktur von Unternehmen können schnell hohe Kosten verursachen, daher spielen Ausfallsicherheit und hohe Verfügbarkeit für den reibungslosen Ablauf des Tagesgeschäfts eine große Rolle. Spezielle Softwarelösungen überwachen die Netzwerkleistung und können im Bedarfsfall auch präventiv durch Benachrichtigungen oder direkte Gegenmaßnahmen Ausfallzeiten auf ein Minimum reduzieren.

Sensoren überwachen die unterschiedlichsten Bereiche der IT-Infrastruktur wie Netzwerk, Windows-Systeme oder Mail-Dienste. Grundlage sind aktive oder passive Abfragen. Die Monitoring-Software Server Sentinel basiert auf der Verknüpfung von Sensoren, Bedingungen und Aktionen. Sensoren sind eigenständige Programmmodule, die unter anderem Server, Dienste, Hardwarekomponenten oder mittels Hardwareunterstützung auch Umgebungseinflüsse wie Raumtemperatur und Luftfeuchtigkeit überwachen.

Die Sensoren lassen sich einzeln mit den für eine Prüfung relevanten Daten konfigurieren. Für die Konfiguration erforderlich sind die Adressaten der Überwachung, in der Regel ein Server-Name, und das Messintervall. Optionale Parameter können zum Beispiel die Zugangsdaten eines zu überwachenden Rechners sein. Die von einem Sensor gesammelten Daten werden nach jeder Messung in einer Datenbank gespeichert.

Zu jedem Sensor lässt sich eine beliebige Anzahl von Bedingungen erzeugen, damit das System auf bestimmte Ereignisse oder Fehler reagieren kann. Dieses kann beispielsweise einen Fehlerzustand oder die Über- oder Unterschreitung eines bestimmten Schwellenwertes (zum Beispiel „weniger als 1 GByte frei“) abdecken. Um eine Bedingung zu überprüfen, wertet die Lösung die jeweiligen Daten eines Sensors als „wahr“ oder „falsch“ aus. Zu jeder Bedingung sind beliebig viele Aktionen für verschiedenste Szenarien konfigurierbar. Dies reicht vom Benachrichtigen der zuständigen Personen per E-Mail oder SMS bis hin zur direkten Einleitung von Gegenmaßnahmen (Failover), durch ein Programm oder Skript.

Aktive oder passive Überwachung

Die Verfügbarkeit von Netzwerksystemen lässt sich aktiv und passiv überprüfen. Bei aktivem Monitoring untersucht die Software in einem definierten Zeitintervall,

ob das zu überwachende System erwartungsgemäß funktioniert. Dabei geht eine Anfrage (Request) an das System. Aus den empfangenen Daten können die für den jeweiligen Sensor relevanten Werte extrahiert werden. Die Einstellung des Zeitintervalls ist besonders wichtig, um eine möglichst lückenlose Überwachung zu gewährleisten.

Im Fall der passiven Überwachung finden keine regelmäßigen Abfragen des zu überwachenden Systems statt. Die Software empfängt lediglich bei Eintreten eines Ereignisses Daten, die das überwachte System von sich aus sendet. Abhängig von der IT-Infrastruktur hat der Anwender die Möglichkeit, aktive oder passive Überwachung mit den gleichen Bedingungen oder Aktionen einzusetzen.

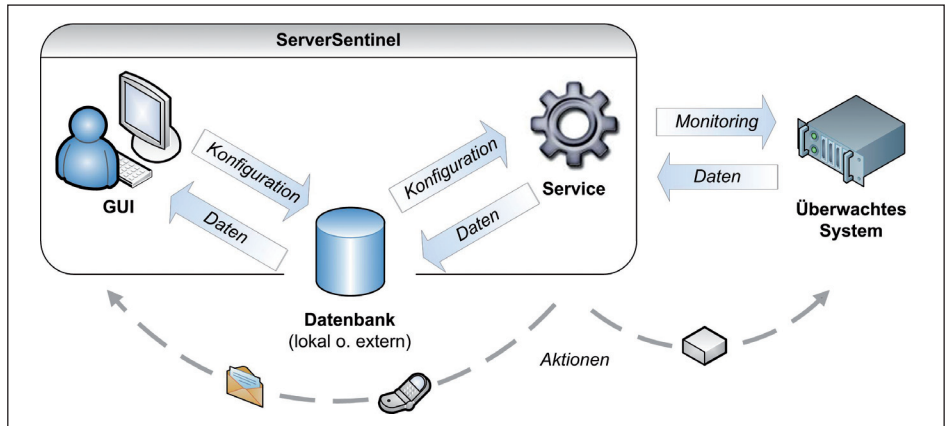
Architektur von Server Sentinel

Die Architektur des hier vorgestellten Systems beruht grundlegend auf drei Komponenten und ihrem Zusammenspiel: der grafischen Benutzeroberfläche (GUI), dem Systemdienst (Service) und der Datenbank. In der GUI sind die Sensoren, Bedingungen und Aktionen intuitiv konfigurierbar. Diese Konfigurationen schreibt das System anschließend in die Datenbank. Der Systemdienst liest die Konfiguration der Sensoren aus der Datenbank und führt entsprechend regelmäßige Abfragen (Polling) durch. Die Ergebnisse der Abfragen laufen in die Datenbank ein. Die GUI greift im Gegenzug auf die gespeicherten Sensordaten aus der Datenbank zu und kann diese beispielsweise noch grafisch als Verlaufsdiagramm darstellen. Die Datenbank stellt somit die Kommunikation zwischen GUI und Service dar. Durch eine Abstraktionsebene, die zwischen Anwendung und Datenbank besteht, sind verschiedenste

Datenbanksysteme leicht zu integrieren. Dies sorgt für eine hohe Datenbankunabhängigkeit.

Ausfallsicherheit im Netzwerk erhöhen

Die häufig genutzten Netzwerksensoren fußen auf dem TCP/IP-Protokollstapel. Die wichtigsten Sensoren für eine effiziente Netzwerk-Überwachung sind ICMP-, SNMP-, HTTP- und TCP-Sensoren. Bei einem ICMP-Sensor (Internet Control Message Protocol), auch als Ping-Sensor bekannt, sind die Reaktionszeit auf eine Abfrage sowie die von der Abfrage gelieferten Daten entscheidend. Server Sentinel löst beispielsweise eine Aktion aus, sobald eine Zeitüberschreitung vorhanden ist, die auf einen Fehler im Netzwerk hindeutet. Der SNMP-Sensor (Simple Network Management Protocol) überwacht aktiv Netzwerkgeräte wie Server, Router, Drucker oder unterbrechungsfreie Stromversorgung (USV) und kann passiv so genannte Traps von diesen empfangen. Traps sind Nachrichten, die über den Eintritt eines Ereignisses informieren, wenn beispielsweise der Strom ausgefallen oder das Papier im Drucker aufgebraucht ist. HTTP-Sensoren überprüfen Web-Server und TCP-Sensoren überwachen beliebige TCP-Ports auf Servern.

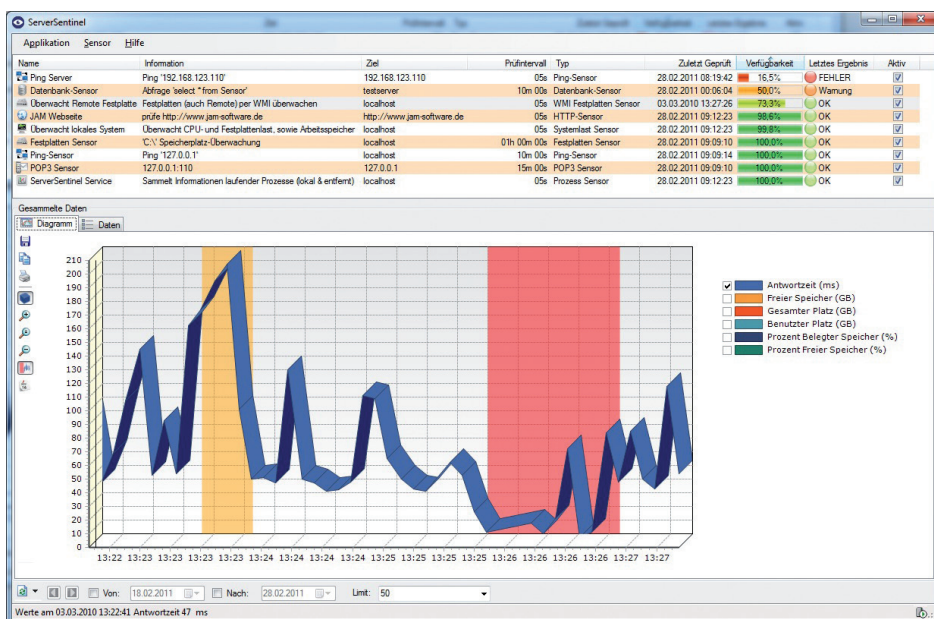


Server Sentinel von Jam Software überwacht Server- und Netzwerkdienste und speichert die gesammelten Informationen in einer Datenbank. Die Software reagiert im Bedarfsfall mit Benachrichtigungen oder aktiven Gegenmaßnahmen.

Mail-Sensoren wie SMTP-, POP3 oder IMAP-Sensoren erlauben es, Mail-Server und deren Dienste zu überwachen. Die Software kann dadurch beispielsweise die Kommunikation mit dem SMTP-Server oder die Verfügbarkeit von POP3-Konten überprüfen, sodass Fehler bei Versand oder Empfang von E-Mails sofort offen erkennbar sind. Ebenso überwacht ein Mail-Sensor, ob bei IMAP-Konten bereits gelesene, ungelesene oder gar keine Mails vorhanden sind. Möglich ist auch eine Prüfung des Mail-Systems mittels Testmail der Monitoring-Software. Windows-Management-Instrumentation-, kurz WMI-Sensoren, können auf Win-

dows-basierenden Systemen arbeiten. Sie ermöglichen Benutzern, eigene Abfragen zu generieren und bieten dadurch ein breites Anwendungsspektrum. Beispielsweise lässt sich auch die Verfügbarkeit von Drucksystemen oder externen Festplatten feststellen. Daneben existieren auch spezialisierte WMI-Sensoren für die Parameter von Festplatten, Prozessen, die Systemlast oder das Windows-Ereignisprotokoll.

Stellt ein Sensor einen Fehler fest, schickt die Software automatisierte Benachrichtigungen per E-Mail oder SMS an den Systemadministrator. Dabei empfiehlt sich, die SMS über ein angeschlossenes Mobiltelefon anstatt über einen Web-Service zu senden, da so eine vom eigenen Netz unabhängige Fehlerübermittlung gewährleistet ist. Neben diesen rein informierenden Aktionen sind auch aktive Aktionen wähl- oder konfigurierbar: Im Fehlerfall führt die Monitoring-Lösung Skripte oder Programme automatisch aus, um Gegenmaßnahmen einzuleiten. Anwenderspezifische Aktionen, die beispielsweise auf Skripten basieren, lassen sich flexibel einbinden. So kann das System sofort auf eine Fallback-Lösung umschalten. Joachim Marder/jos



Alle konfigurierten Sensoren lassen sich im Hauptfenster betrachten. Darunter erscheinen die gesammelten Daten in Listen- und Diagrammform.

Joachim Marder ist Geschäftsführer und Inhaber von Jam Software.

Info: JAM Software GmbH
Tel.: 0651/145653-0
Web: www.jam-software.de